NENA
Security for Next-Generation 9-1-1 Standard
(NG-SEC)

NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
NENA 75-001, Version 1, February 6, 2010

Prepared by:
The National Emergency Number Association's (NENA) Security for NG9-1-1 Working Group; a joint working group of the CPE Committee and the Next Generation Integration (NGI) Committee.

Published by NENA
Printed in USA

NENA STANDARD DOCUMENT

NOTICE

The National Emergency Number Association (**NENA)** publishes this document as a guide for the designers and manufacturers of systems to utilize for the purpose of processing emergency calls. It is not intended to provide complete design specifications or to assure the quality of performance of such equipment.

NENA reserves the right to revise this NENA Standard for any reason including, but not limited to:

- conformity with criteria or standards promulgated by various agencies
- utilization of advances in the state of the technical arts
- Or to reflect changes in the design of equipment or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this NENA Standard should not be the only source of information used. **NENA** recommends that readers contact their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: nrs-admin@nena.org

Acknowledgments:

The National Emergency Number Association (NENA) Joint CPE Committee and Next Generation Integration (NGI) Committee developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Version [1], Approval Date, [02/06/2010]

Members	**Company**
Smith - CISSP, Jeremy, WG Co-Leader	L R Kimball
Vanauken-ENP, Gordon, WG Co-Leader	L R Kimball
Allocco, Jim	Spectracom Corporation
Armstrong, Mike	Verizon
Boyken, Bill	AT&T
Corprew, Charles	AT&T
Dantu, Ram	
Davis, Kenneth	Sangamon County ETSD
Dilday, Clay	North Central Texas Council of Govt.
Erdman, Bob	Amcom Software
Frye, Richard T	FRYE-COMM Consulting LLC
Good, Travis	Center for Infrastructure Assurance and Security
Harry, William	
Hayes, David W	L R Kimball
Humrich, Timothy	Qwest
Irons, Johnny	9-1-1 ACOG
Irwin, Dave	Washington Military Department, Emergency Management Division
Jones-ENP, Rick	NENA
Kaczmarczyk, Casimer M	Verizon
Kleck, Kevin	Tarrant County 9-1-1 District
Kleckner, Lori	State of Missouri
Lagreid, Steve	King County, E9-1-1 Program.
Lewis, Shelby	Positron
Lipinski, Jim	State of Vermont
Maroney, Craig	EMC LLC
Mathis, CISSP ENP PSNP, Ron	Intrado Inc.
McClure, ENP, Nate	CTA Communications
McIntire, Clay	North Central Texas Council of Governments

Moody, Martin D	Metro Emergency Services Board
Oenning, Bob	State of Washington
Ogletree, Brett	
Payne, Mark	Denco Area 9-1-1 District
Porter, RD	State of Missouri
Range, Bill	Dept of Finance and Administration, State of New Mexico
Rosen, Brian	NeuStar
Schlesinger, Jerry	RCC Consultants, Inc.
Seet, Susan M	Texas Commission on State Emergency Communications (CSEC)
Skain, John	Clinton County 9-1-1
Slivka, Joe Ben	Summit County Communications Center
Stork, ENP, Maureen	
Sylvester, Robert L.	Convergent Technologies, Inc.
Thakur, Vikram	
Tschofenig, Hannes	Nokia Siemens Networks
Vick, Chuck	Verizon Business
Vislocky, Mike	Network Orange, Inc.
Walthall, CISSP, Robert	AT&T
Whitehurst, William Ron	Cbeyond Communications
Wilcox, Nathan G	microDATA
Williams, Dwayne	CIAS
Winegarden, Jim	Qwest Communications
Wise, Marc	AT&T

This working group would also thank Tom Breen, Technical Committee Chair/Liaison; Tony Busam, Technical Committee Vice-Chair/Liaison; Pete Eggimann, Operations Committee Chair/Liaison; Wendy Lively, Operations Committee Chair/Liaison; Roger Hixson, Technical Issues Director; and Rick Jones, Operations Issues Director for their support and assistance. Additionally, the working group would also like to give a special thank you to Barbara Thornburg whose assistance in formatting was exceedingly helpful.

TABLE OF CONTENTS

1 Executive Overview

Purpose

The purpose of this document is to establish the minimal guidelines and requirements for the protection of NG9-1-1 assets or elements within a changing business environment.

This document:

- Identifies the basic requirements, standards, procedures, or practices to provide the minimum levels of security applicable to NG9-1-1 Entities.
- Provides a basis for auditing, and assessing levels of security and risk to NG9-1-1 Entities, assets or elements, and exception approval / risk acceptance process in the case of non-compliance to these guidelines.

Scope

This document is applicable to all NG9-1-1 Entities including, but not limited to:

- Public Safety Answering Points
- NG9-1-1 “ESINet”
- NG9-1-1 Service Providers
- NG9-1-1 Vendors
- Any Contracted service that perform functions or services that require securing NG9-1-1 assets.
- Those who use, design, have access to, or are responsible for NG9-1-1 assets (includes computers, networks, information, etc.).

2 Introduction

2.1 Operational Impacts Summary

This document will impact the operations of 9-1-1 systems and PSAPs as standardized security practices are implemented where they have not been in place before. NG9-1-1 Entities will be required to understand, implement and maintain new security solutions, mechanisms and processes.

2.2 Security Impacts Summary

This Security standard may impact other NENA standards and should be reviewed by each committee.

2.3 Document Terminology

The terms "shall", "must" and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words “should,” "desirable" or "preferably".

2.4 Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Version	Approval Date	Reason For Changes
Original		Initial Document

2.5 Recommendation for Additional Development Work

Security is an evolving process and this document should be reviewed on a regular basis for changes.

2.6 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

To ensure true compliance, the manufacturer shall upon request, provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

2.7 Anticipated Timeline

Applicable sections of this standard should be implemented immediately. NG9-1-1 entities who implement NG9-1-1 components, parts, or solutions must implement all applicable sections of this standard.

2.8 Costs Factors

This standard will have a cost impact to the entities that are impacted. NG9-1-1 Entities are encouraged to expand budgets to specifically include costs related to compliance with this standard.

2.9 Future Path Plan Criteria for Technical Evolution

In present and future applications of all technologies used for 9-1-1 call and data delivery, it is a requirement to maintain the same level or improve on the reliability and service characteristics inherent in present 9-1-1 system design.

New methods or solutions for current and future service needs and options should meet the criteria below. This inherently requires knowledge of current 9-1-1 system design factors and concepts, in order to evaluate new proposed methods or solutions against the Path Plan criteria.

Criteria to meet the Definition/Requirement:

1. Reliability/dependability as governed by NENA's technical standards and other generally accepted base characteristics of E9-1-1 service
2. Service parity for all potential 9-1-1 callers

3. Least complicated system design that results in fewest components to achieve needs (simplicity, maintainable)
4. Maximum probabilities for call and data delivery with least cost approach
5. Documented procedures, practices, and processes to ensure adequate implementation and ongoing maintenance for 9-1-1 systems

This basic technical policy is a guideline to focus technical development work on maintaining fundamental characteristics of E9-1-1 service by anyone providing equipment, software, or services.

2.10 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism.

2.11 Additional Impacts (non cost related)

Not Applicable.

2.12 Intellectual Property Rights Policy

NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: techdoccomments@nena.org

2.13 Acronyms/Abbreviations

Some acronyms/abbreviations used in this document have not yet been included in the master glossary. After initial approval of this document, they will be included. See NENA 00-001 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents. Moreover, some acronyms already existing the NENA Master Glossary but shall be updated as noted below. Wikipedia.com was used as a reference for many of these acronyms.

The following Acronyms are used in this document:		
Acronym	Description	** N)ew (U)pdate
(none)		

3 Technical Description

3.1 Severity Categories

Determining whether entities comply with the security requirements stated herein requires an audit to determine compliance. This process is made easier through the definition of severity categories (e.g. High, Medium, or Low) that can be used as a guide for auditors and risk assessors. In this first release of the standard, NENA chose not to include severity categories. It is anticipated that NENA may release a future version of this document that will contain severity categories that would be helpful for auditing and compliance purposes. In the interim, periodic audits are still required as noted later in this document in section 11. NG9-1-1 Entities are required to comply with all applicable portions of the standard.

3.2 Statement of Compliance

Use of the information contained within this document, to develop detailed security requirements, standards, procedures, and practices is recommended for all NG9-1-1 Entity owned infrastructure and devices, in order to provide minimal protection for NG9-1-1 assets and the information and assets of others.

Once detailed security requirements, standards, procedures, and practices are developed by the vendor, non-compliance shall be documented to identify security vulnerabilities, determine associated criticality, and establish a compliance action plan.

Unresolved non-compliance that introduces risk to NG9-1-1 shall require documented risk acceptance as described in Section 12, Exception Approval/Risk Acceptance Process.

3.3 Roles & Responsibilities

An effective security program involves many different roles and responsibilities within, and external to, the NG9-1-1 Entity. Some common roles are listed below (Some roles may be fulfilled by same person).

- **Senior Manager:** Executive or other department manager ultimately responsible for the security of the organization and may be responsible for the operation of all data processing, network, and access to all IT operations of the NG-911 Entity. This person or their designated representative will define security policy as it relates to all systems, networks, and data for the NG9-1-1 Entity as a whole. Many times, this role could be defined and identified by legal statute or regulation.

- **Security Administrator**: Has the functional responsibility for organizational security and is responsible for implementing and administrating security countermeasures in concordance with NG9-1-1 security policies.
- **Data Owner**: Is responsible for appropriately classifying the asset or helping the NG9-1-1 Entity understand its importance in order to establish the necessary level of protection.
- **Data Custodian**: Responsible for ensuring that any security measures required for a particular asset are implemented and maintained.
- **Data User**: The entity that actually uses the data being secured. For example, the Dispatcher is a Data User in that they 'use' ALI data to perform their daily tasks.
- **Auditor**: Auditors may be internal or external to the organization and are responsible for examining an organization's security.

Safeguarding the assets of the organization, both physical and data, is everyone's responsibility and every individual within the NG9-1-1 Entity should be educated and included in the NG9-1-1 Entity's security 'mindset.'

4 Security Policies

The creation of a security policy is the first step in any effective attempt at implementing a security program. A Security Policy is a clearly documented statement of organizational goals and intentions for security, particularly upper management's commitment to Security. The creation of a security policy requires an organization to recognize, identify, and document its commitment to security. All too often organizations implement security measures without first implementing security policies. This often results in ineffective or unfocused security controls and ultimately leads to more vulnerability. A security policy should facilitate an environment of secure computing and document an organization's philosophy concerning security.

Security policies vary in size and shape as well as purpose or scope.

At a minimum, an organization shall have the following policies as part of a security program:

- Senior Management Statement of Policy (sometimes called an Organizational Security Policy)
- Functional Policies
- Procedures

4.1 Senior Management Statement of Policy

NG9-1-1 presents new threats and risks. Senior management must be engaged and committed to maintain highly effective security so the rest of the staff can be able to do their part. Security cannot be made someone else's responsibility; everyone, and especially management, must be involved and vigilant. Creating a senior management statement of policy is crucial to documenting the importance of the computing assets and resources to the organization as well as upper management's commitment to exercise due care through the definition and management of acceptable operational level standards, procedures, and measures.

The Senior Management Statement of policy shall, at a minimum:

- Indentify person responsible for security
- Provide a written description of the security goals and objectives of the NG9-1-1 Entity

4.2 Functional Policies

Functional policies provide a deeper level of granularity after creating an executive management statement of policy. Functional policies must be established prior to the implementation of any actual security measures. Some examples of functional policies include:

- Acceptable Usage Policy (i.e. email, Internet usage, USB storage device, personal computer use, blogging, social networking, etc)
- Authentication/Password policies
- Data Protection Policy
- Wireless Policy
- Physical Security Policy
- Remote access policies
- Hiring practices
- Security enhancements or technology that should be implemented within a NG9-1-1 Entity
- Baseline configurations for workstations existing on the NG9-1-1 Entity network
- Standards for technology selection
- Incident Response Policy

4.3 Procedures

A procedure is the documented method of performing a specific task. As an organization's security policies begin to take shape it will become necessary to document certain tasks such as the procedures on creating new user accounts or the actual steps to allow a vendor access to a server room. Procedures are an important part of any security strategy because they take the guesswork out of certain tasks ensuring consistency and accountability.

5 Information Classification and Protection

5.1 Overview

Information classification is the framework for evaluating and protecting information and assets that contain information owned and used by the NG9-1-1 Entity. Information is categorized based on the sensitivity, applicable policies and/or legal and statutory requirements.

5.2 Roles and Responsibilities in Information Classification and Protection

5.2.1 Data Owner

When a vendor, NG9-1-1 employee, contractor, agent or service provider creates a document, or is designated responsible for a system, device or media containing sensitive information, he/she shall become the data owner of/for it. The data owner responsibilities include:

- Judging the value of the information resource and assigning the proper classification level according to this guideline.
- Periodically reviewing the classification level to determine if the status shall be changed.
- Communicating access and control requirements to the data custodian and users.
- Providing access to those individuals with a demonstrated business need for access.
- Assessing the risk of loss of the information and assuring that adequate safeguards are in place to mitigate the risk to information integrity, confidentiality, and availability.
- Monitoring safeguard requirements to ensure that information is being adequately protected.

5.2.2 Data Custodian

When a vendor, NG9-1-1 Entity employee, contractor, agent or service provider retains Sensitive information, he/she shall become a custodian of that information and is responsible for protecting its confidentiality, integrity and availability according to the rules and regulations established by the originator. At a minimum, the custodian is responsible for:

- Complying with information classification and protection policies on retention and disposal of records and information.
- Providing proper safeguards for the information, including following guidelines in this Guideline for proper disposal. In those cases where information must be printed from electronic media, the custodian must mark the printed information with the appropriate classification.
- Providing proper safeguards for processing equipment, information storage, backup, and recovery.
- Providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.
- Administering access requests to information properly authorized by the originator.
- Using the information only for the purpose intended.
- Maintaining the integrity, confidentiality, and availability of information accessed.

Being granted access to information does not imply or confer authority to grant other users access to that information beyond the normal boundaries established for a given classification. This is true whether the information is electronically held, printed, hardcopy, manually prepared, copied, or transmitted.

5.3 Information Classification Guidelines

Information Classification defines four (4) classifications for information owned or used by the NG9-1-1 Entity as defined later in this document:

- Public
- Sensitive (Internal Use Only)
- Sensitive (Restricted)
- Sensitive (Most Sensitive Information)

NOTE: While other levels or classifications may exist, they may be specific to each organization and therefore, not listed here.

5.4 Protecting Sensitive Information

5.4.1 Classifying Information

NG9-1-1 Entity uses information that it owns as well as information owned by other persons or entities.

NOTE: Information that is proprietary to another company or government agency shall be obtained legally with the agreement of the other company or agency and in compliance with the appropriate code of conduct. Information shall be classified using the highest applicable classification based upon the descriptions below.

Examples of each type of information follow this section and are separated into NG9-1-1 Entity information, and non-NG9-1-1 Entity information (e.g., service provider, third party, and government entities information), and public information.

This section is intended to serve as a guideline to organizations seeking to classify their information. NG9-1-1 entities should ensure they comply with all applicable laws and regulations such as the Freedom of Information Act (FOIA).

The security policy of the NG9-1-1 Entity shall specify which classifications of data it believes are not subject to FOIA.

5.4.2 Public

1. Description
   a. Information for which there is no value in keeping it secret, or
   b. Information intended for public disclosure and purposely placed in the public domain, or must be made publicly available per applicable policies, and/or legal and statutory requirements
      1. Does not necessarily imply that the information must be made public

2. Examples of Public Safety Information

   a. Guidance for ordering products and services (i.e. Vendor Product Briefs, RFPs, etc)
   b. Public directory information (i.e. Phone number to Police Department)

3. Examples of non-Public Safety Information
   a. Any public domain information (i.e. website addresses, etc)

5.4.3 Sensitive (Internal Use Only)

1. Description
   a. Information that is sensitive and not intended for public disclosure, whose value could be diminished if publicly disclosed, or
   b. Information that could be valuable to create unintended obligations or liabilities for Public Safety if revealed outside Public Safety domain, or
   c. Information that is intended for all employees or authorized contractors or is of such a nature that it is in Public Safety organization's interest to allow any employee to determine if there is a legitimate need to share it with any other employee.

2. Examples of Public Safety Information
   a. Internal directory entries excluding fields specifically identified in other classification levels,
   b. General Process and Operational information,
   c. Service Descriptions,
   d. Internal communications and instructions,
   e. Policies, Standards and Guidelines.
   f. Data relating to Internet usage

3. Examples of non-Public Safety Information
   a. The same type of information owned by the service provider and third party including government entities.

5.4.4 Sensitive (Restricted)

1. Description
   a. Information that has a higher level of sensitivity and which the originator determines shall be shared only among specifically identifiable persons or team with a clear need to know, or
   b. Information that requires a high degree of protection by law and loss or unauthorized disclosure could require notification by Public Safety to government agencies, individuals or law enforcement, or
   c. Information, that if revealed widely within Public Safety could present an increased risk of compromising computer systems, fraud, or increased probability of disrupting the day to day operation of the Emergency Communication System.
   d. Not intended for public release

2. Examples of Public Safety Information
   a. Strategic Operational plans including Fall-Back sites, Fuel Depots, etc.
   b. Personnel and salary information
   c. Internal Audit information
   d. Security information including logs, authentication credentials (passwords and pins), architecture diagrams, and configuration files
   e. Network information including engineering or architecture diagrams and configuration files related to IT networks
   f. Research and development information including studies, designs and development plans for new or improved products, services, or processes
   g. Incident reports and vulnerability
   h. Attorney-Client Privileged information
   i. Customer Proprietary Network Information (CPNI) as described in the US Telecommunications Act of 1996
   j. Firewall rules
   k. Software source code for critical applications.

3. Examples of non-Public Safety Information
   a. The same type of information owned by Service Provider or third party including government entities.

5.4.5 Sensitive (Most Sensitive Information)

1. Description
   a. Information that requires a high degree of protection by law and loss or unauthorized disclosure would require notification by Public Safety to government agencies, individuals or law enforcement, and
   b. Information that, if made public, could expose NG9-1-1 entities to a risk of physical harm, compromise of undercover operations, public safety operations, fraud or identity theft, etc.

2. Examples of Sensitive (Most Sensitive Information)

The following “Privacy” data elements have been classified as Sensitive (Most Sensitive Information):

Individual Identification	
Data Element	**Description**
NG9-1-1 Entity User Identification Value	Specific NG9-1-1 Entity UID Value (that are used as a data element, not as a login) shown in association with owner
Drivers License Number	

Nationally-Issued Identification Number	Includes visa and/or passport values
State or Province-Issued Identification Number	
Social Security Number (SSN)	Includes any portion of SSN
Computer Identification and Authentication	
Description	
PINs, Passwords or Passcodes	Values used by a user to allow (authentication of) access to public safety information or service, includes calling card PINs and secret codes
Stored Password Hint Answers	Answers to questions used to retrieve passwords, for example mother's maiden name

Other Data	
Data Element	Description
Date of Birth (DOB)	Includes month, day and year
Biometric Data	Measures of human physical and behavioral characteristics used for authentication purposes, for example voiceprint, retina or iris image, also includes scanned images.
Digitized or Electronic Signatures	A digital representation of a manual signature
56BBackground Check Data	Results of background check
Information obtained from NCIC (National Crime Information Center)	NCIC is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, and missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year.
Medical Information	Personal medical information
ALI and ANI information	Phone numbers and addresses

5.4.6 Receipt of Sensitive Information

Sensitive information received from external parties shall be clearly marked by the recipient as sensitive and treated in accordance with any applicable regulations or restrictions (such as those set forth in a contract between NG9-1-1 entities and a Service provider, etc).

The sensitive information of Service Providers or third parties, including government entities, shall, unless otherwise specified in the contract with Service Providers or the third party, be safeguarded in the same manner as NG9-1-1 Entity information of like sensitivity or pursuant to Nondisclosure Agreements in place which may govern handling of such data or local, state or federal laws governing sensitive data.

5.5 Default Classification

If the classification of information is unknown, the information shall be treated as Sensitive (Internal Use Only) until the proper classification is determined or it is determined to be Public Information by the originator or other applicable laws and regulations.

5.6 Authorizing Access to Information

All access to information by any service provider, vendor, NG9-1-1 Entity employee or contractor shall comply with applicable codes of conduct, policies, contracts, laws and regulations. Persons not authorized to view or modify information shall be prohibited from viewing or modifying information.

Persons who are not NG9-1-1 Entity employees (e.g., contractors, suppliers, or vendors) shall have appropriate contractual agreements in place that establish their relationship to the NG9-1-1 Entity and authorize their access to NG9-1-1 Entity resources prior to being granted access to information of any classification other than Public.

5.6.1 Public

Public information may be shared with anyone inside or outside the service provider, vendor, or NG9-1-1 Entity and may be presented or published in the public domain.

5.6.2 Sensitive (Internal Use Only)

Internal Use Only information may be shared with any employee with a legitimate need, and may be shared with any non-payroll worker (e.g., contractor) who is authorized.

Release of Sensitive (Internal Use Only) information shall be documented when released subject to an FOIA request.

5.6.3 Sensitive (Restricted)

Restricted information shall be shared only with the explicit permission of the originator. Permission shall be in writing. Electronic communication is acceptable. Electronic systems that support the notion of role-based approval or rights based responsibilities are allowable.

Release of Sensitive (Restricted) information shall be documented when released subject to a FOIA request.

5.6.4 Sensitive (Most Sensitive Information)

Most Sensitive Information shall only be shared or modified with the explicit permission of the originator and/or in accordance with applicable laws and regulations. Electronic systems that support the notion of role-based approval or rights based responsibilities are allowable.

Release of Sensitive (Most Sensitive) information shall be documented when released subject to an FOIA request.

5.7 Safeguarding Electronic Information

Where **Sensitive (Most Sensitive Information)** data is allowed to be stored or transmitted on a network between devices, whether inside or outside the NG9-1-1 Entity it must be encrypted. In NG9-1-1 systems, the encryption algorithm shall be AES.

Where Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) data stored on removable or portable media (such as USB flash drives, thumb drives, memory sticks, external hard drives, or CDs), and mobile computing devices (such as laptops, PDAs or blackberries), it:

Shall either be kept in the direct supervision of the custodian or physically secured from unauthorized access (e.g., in a locked office, desk, or filing cabinet), and

Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., shall not be placed in taxi trunk/boot, bus hold/baggage storage, checked-in on airplane).

However, mobile computing devices containing Sensitive (Most Sensitive Information) shall not be taken outside NG9-1-1 Entity controlled space, but if there is an overriding business need to do so then approval shale documented in policies that allow applicable roles to have such rights. Exceptions to the policy shall be documented in writing.

Whenever systems containing vendor, service provider or NG9-1-1 Entity information requires repair, the service provider or vendor employees and contractors shall use only approved repair processes, groups or locations and in accordance with applicable non-disclosure agreements, laws, regulations and policies to ensure that information contained on the devices is safeguarded in keeping with its sensitivity level.

5.8 Transport and Shipping of Electronic Media and Devices

Media or devices containing Sensitive (Most Sensitive Information) **shall** be hand delivered by the custodian. However, if there is an overriding business need to do otherwise then approval **shall** be obtained from a senior Manager and be shipped in sealed packages utilizing recorded/certified delivery.

Media or devices containing sensitive information, other than Sensitive (Most Sensitive Information), shall be shipped in sealed packages either via interdepartmental mail or utilizing recorded/certified delivery via a mail delivery service.

5.9 Safeguarding Printed Information/Material

5.9.1 Sensitive (Internal Use Only) – Printed Material

1. Inside Controlled Space:
   a. Shall be kept away from visitors who have no need to see the information
   b. No Controls required when distributed within the controlled space
   c. Shall supervise sending and receiving fax machines with authorized personnel, or use fax machines in offices/areas where access is limited to authorized personnel.
   d. Shall be shredded after use

2. Outside Controlled Space:
   a. Shall be secured from unauthorized access
   b. Shall be kept in the direct supervision of the custodian
   c. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage)
   d. Shall supervise the printer or copier with an authorized person for the information
   e. Shall use a sealed envelope whenever delivery is to a location external to the controlled space or whenever the delivery utilizes non-company personnel or service.
   f. Shall supervise fax machines that are located outside the controlled space with authorized personnel.
   g. Shall be shredded after use

5.9.2 Sensitive (Restricted) – Printed Material

1. Inside the Controlled Space:
   a. Shall be kept away from casual observers.
   b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe).
   c. If the controlled space is only accessible to the designated "Team", it is not necessary to keep hidden or physically secured when unattended.
   d. Shall either supervise the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
   e. Shall be hand delivered by originator or custodian.
   f. Shall use double envelopes with the inner envelope marked "Private" when using internal mail.
   g. Shall supervise sending and receiving fax machines with authorized personnel, or use fax machines in offices/areas where access is limited to authorized personnel.
   h. Shall use special bins provided or be shredded

2. Outside the Controlled Space:
   a. Shall be kept away from casual observers.
   b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
   c. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., taxi trunk/boot, bus hold/baggage storage, checked baggage on airplane).
   d. Shall supervise the printer or copier with a person authorized for the information.
   e. Shall use double envelopes with the inner envelope marked "Private" and send recorded/certified delivery whenever delivery is to a location external to controlled space or whenever the delivery utilizes non-company personnel or service.
   f. Shall supervise fax machines that are located outside NG9-1-1 Entity controlled space with authorized personnel.
   g. Shall be shredded

5.9.3 Sensitive (Most Sensitive Information) – Printed Material

1. Inside the Controlled Space:
   a. Shall be kept away from casual observers.
   b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe).
   c. Shall either supervise the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
   d. Shall be hand delivered by the originator or custodian.
   e. Shall not be faxed.
   f. Shall be shredded.

2. Outside the Controlled Space:
   a. Shall never be taken outside the controlled space.
   b. If there is an overriding business need then:
      1. Shall obtain approval from a Senior Manager.
      2. Shall be kept away from casual observers.
      3. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
      4. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., taxi trunk/boot, bus hold/baggage storage, checked baggage on airplane).
      5. Shall not print/copy outside the controlled space. Or shall supervise the printer or copier with a person authorized for the information.
      6. Shall hand deliver by the data owner or data custodian.
      7. Shall not be faxed.
      8. Shall be shredded.

5.10 Sensitive Information Destruction & Sanitization

5.10.1 Hard Copies or Printed Material

When hard copy Sensitive documents are no longer needed or required to be retained, they shall be properly disposed.

Some locations will have special locked "sensitive material" bins (which prevent access to documents once inserted) where documents may be left. These bins shall be periodically emptied and the contents taken away for secure shredding.

Where "sensitive material" disposal bins are not available, shredding shall be performed. Shredding shall be done in such a way that it is impractical to reconstruct either the whole document, or a large enough part, from the pieces such that the information contained on it might be compromised. The recommended approaches being to either use cross-cutting into pieces/confetti (width (max): 3/4 inch or less and length (max): 2.5 inches or less) or continuous cutting/shredding into strips (width max: 5/8 inch or less and length: indefinite or less).

5.10.2 Sanitizing Media or devices whose media contains Sensitive data, e.g., PCs, CDs, Hard disks, Tapes, USB drives

All media types shall have Sensitive information sanitized (rendered irretrievable), in a manner that will prevent misuse or unauthorized disclosure prior to repair, reuse or disposal. It is well known that even after data has been deleted or moved the data may actually still reside on the device. This is because many operating systems do not actually erase the data, but only remove the pointers between the directory and the data locations. This may result in the data being accessible by unauthorized person(s) using readily available utility programs.

Examples of media sanitization approaches include:

- Degaussing
- Magnetic Media Erasing
- Disintegrators
- Optical Media Destruction
- Disk Erasers
- Services that offer media destruction

6 General Security

6.1 General Responsibilities

Agreements between the NG9-1-1 Entity and vendors, contractors or suppliers for the purchase, development, or support of information resources or services shall incorporate the appropriate contractual security requirements, detailed roles and responsibilities (including Application, System and Network Administrators) and applicable security review or assessment to ensure the protection of all relevant information, systems, and services. “Information resources” shall include any owned or managed systems, applications, and network elements, and the information stored, transmitted, or processed with these resources.

Contractors, suppliers and supplier’s employees and subcontractors shall protect information resources in accordance with the terms and conditions of applicable contractual agreements between the contractor or supplier and NG9-1-1 Entity.

In addition, it shall be the responsibility of all contractors, suppliers and supplier’s employees and subcontractors to comply with applicable federal, state, and local acts, statutes, and regulations that relate to the control and authorized use of information and information resources.

These requirements apply to the entire supplier or supplier subcontractor environment that may impact the information resources used to support the contract.

6.2 Application, System and Network Administrator Responsibilities

Application, system, and network administrators shall perform self-review on the systems for which they have operational responsibility at least once a year to ensure that the systems are compliant with all security requirements. These assessments shall be in writing and communicated to the designated security manager and NG9-1-1 Entity management. Entities may choose to outsource the self-review activity to designated IT security firms as noted in section 11 of this document.

A copy of current security self-reviews or security assessments/audit reports shall be retained for future reference and audit purposes until superseded by another security assessment or until the system is retired.

6.3 Ensuring Compliance for Recurring Security Requirements

The applicable Application, System and Network Administrator shall identify which security solutions have or require periodic review. For example: Intrusion Prevention Systems, Event Logs.

The applicable Application, System and Network Administrator shall implement and execute a plan to periodically review items identified in preceding section and take appropriate action.

6.4 Network Connectivity Requirements

6.4.1 General

Network security forms a cornerstone of the overall security posture for any NG9-1-1 Entity and connecting entities. An improperly secured network can present many problems to an NG9-1-1 Entity such as providing an avenue for intrusion by unauthorized machines or personnel, loss of service including an inability to accept critical calls from the public or a conduit for propagation of malicious or destructive code. While no network can be declared totally secure, there are measures that can be taken to significantly improve the overall security of a given network. The next few sections will provide requirements for improving network security.

6.4.2 Purpose

When architecting networks it is useful to clearly define a purpose or mission for any given network so that the appropriate security measures can be implemented

6.4.3 Inventory

An accurate and current inventory is a key requirement for network security. Such an inventory will provide a basis for comparison to detect unauthorized devices which may appear on the network. All devices in the inventory shall comply with other aspects of this and other relevant guidelines. Various tools exist which can assist with the creation of an accurate inventory and provide an assessment of the security compliance of various platforms on the network. Inventories shall be classified appropriately and in accordance with the implemented information classification and protection policy.

6.4.4 Controlling Points of Access

All administrative access to any network shall be precisely controlled with appropriate identification, authentication and logging capabilities. All points of ingress and egress to a network shall be fully documented, approved and protected. Such points may include but are not limited to the following: modems, dual- homed platforms, wireless routers or access points, routers and firewalls or gateways. Even different network technologies shall be clearly documented such as those used for "out of band" access, typically for operations access. Points of access that do not support the objectives of the call center shall be eliminated. Remaining points of entry shall be controlled. Many technologies exist for this purpose including firewalls, intrusion detection and prevention devices, proxies, etc. In no case shall any uncontrolled point of entry or "gateway" be permitted on a network.

For standards relating to Remote Access see section 9.

6.4.5 Use of Dual or Multi-Homed Device

A dual or multihomed computer is a host (this does not refer to routers, firewalls, switches, etc, in this context) connected to two or more networks or having two or more network addresses. For example, a call taking computer may have a network interface connected to a CPE network and another connected to a CAD network.

Multihoming computers for vendor convenience and isolating problems introduces security risks and creates avenues for malicious code to more easily spread amongst the networks as well as making the network configuration more complex. Therefore, multihomed computers should be avoided. Instead, if business requirements dictate that a computer must access resources resident on different networks, the networks should be connected together and the appropriate security countermeasures, including those described in this document, should be implemented.

When multihoming computers cannot be avoided, the following guidelines are provided:

- Connecting multihomed computers to networks that have differing security postures shall not be allowed. For example, one network utilizes antivirus software while the other network does not.
- Operating Systems should be hardened
- Application should be hardened
- Anti-virus running on both networks and on multihomed computer
- Host Intrusion Prevention Software (IPS) running on multihomed computer
- IP-forwarding explicitly disabled
- Other appropriate security countermeasures, including those described in this document should be implemented

Important Note: The preceding sections do not apply to, affect or eliminate the need or capability for a computer to utilize more than one network interface card connected to the *same* network for redundancy purposes (i.e. Network Interface Card Teaming for bandwidth aggregation, failover, and/or isolated tape backup or management network specifically for system administration purposes).

6.4.6 Wireless access

Wireless networks do not utilize cable media (ex. Ethernet, COAX) to transmit signals for carrying data. Typically, wireless networks utilize radiated power or radio signals of various formats. Since these signals are not confined to a physical space such as building walls, security measures must be taken to manage risks associated with wireless media. The following sections will list common types of wireless network technologies and provide requirements and recommendations for securing them.

6.4.6.1 802.11 LANS – (802.11 a.b.g.n.)

Wireless Local Area Networks, hereafter referred to as 802.11 LANs, are networks that allow for LANs to be deployed using wireless technologies such as 802.11g, 802.11b, etc. 802.11 LANS shall not be deployed without the following security measures in place under any circumstances. 802.11 LANS shall implement the following at a minimum:

- Default router management password shall be changed and treated as administrator level passwords for syntax, history and periodic changes
- Router management over the wireless link shall be disabled. Router management shall use an encrypted protocol (ex https) whenever available.
- Service Set Identifiers (SSID) shall be changed from default value to an identifier not easily associated with the NG9-1-1 Entity or otherwise easily guessed.
- SSID broadcast shall be disabled
- Wireless security (encryption) shall be enabled. Wired Equivalent Privacy (WEP) shall not be used. 802.11 Protected Access (WPA) or greater (WPA2 with AES and Temporal Key Interchange Protocol (TKIP) 802.11i) is required.

- TKIP passphrase shall be non-trivial and meet minimum length and complexity requirements defined in this document for passphrases.
- Rekey interval shall be 3600 second maximum.
- The 802.11 LAN shall be dedicated to the NG9-1-1 Entity and not shared with any other user community (such as public LANS).
- Media Access Control (MAC) address filtering shall be enabled and the MAC filter list shall be reviewed and purged at a minimum of monthly and immediately whenever a machine is retired from the network. .

Ad hoc modes shall be disabled.

802.11 LANS should consider the following additional measures to minimize risks.

- Maximum encryption key lengths supported by the device should be utilized
- Router Dynamic Host Configuration Protocol (DHCP) services should be disabled and require static Internet Protocol (IP) Addresses for connected devices. If DHCP must be used, the DHCP scope (range of addresses) should be kept to a minimum length.
- If DHCP is used, automatic assignment of other services (e.g. DNS servers, WINS servers) is allowed and should be reviewed in concert with the overall security plan.
- The default SSID channel should be changed from its default value.
- The 802.11 LAN hardware should utilize a third party authentication service for management (such as TACACS, Radius) when supported.
- The 802.11 LAN should utilize a Network Access Control (NAC) technology to ensure proper patching and malicious software screening is performed on all LAN assets. At a minimum, use of a rogue device detection capability is STRONGLY recommended. Also, use of Intrusion Detection Systems (IDS) is encouraged on 802.11 LANs.
- The 802.11 LAN should be separated from other networks by a firewall which limits access to and from the wireless network on an exception basis only.
- Users should be authenticated to the wireless LAN using a two factor mechanism or emerging authentication standards like 802.1x.

6.4.6.2 Bluetooth Networks and similar short range device-specific proprietary wireless networking solutions

Bluetooth is an open wireless protocol for exchanging data over short distances from fixed and mobile devices thus creating personal area networks (PANs).

- Bluetooth wireless networking should be avoided where possible, including wireless headsets and other human interface devices such as mice and keyboards.
- Bluetooth shall not be used for “backups” for any medium or device which contains sensitive (internal data only) or greater data.
- Bluetooth, if used, must be configured to require device identifiers.
- Presence of frequency hopping, phase shifting, device serialization or other such technologies alone shall not satisfy encryption or identification requirements.

6.4.6.3 Broadband Wireless Connections

In 2002 the FCC designated 50 MHz of spectrum in the 4940-4990 MHz band for use in support of public safety. A license from the FCC must be obtained in order to utilize the 4.9 GHz band.

The FCC has approved any terrestrial based radio transmission including data, voice, and video - including Point-to-Point and Multipoint operations for use in this spectrum. Current deployments include: Wireless LANs for incident scene management, Mobile data, Video security, VoIP, PDA connectivity, Hotspots, and T1 line replacement or redundant WAN links.

The requirements and guidelines specified in NG-SEC apply to all communications in the 4.9G MHz band. All communications over this band should be encrypted. Authentication, authorization, and accountability should be maintained. Firewalls shall be deployed at network boundaries.

6.4.6.4 Broadband wireless technologies for mobile users (e.g. Laptop, handheld and other devices)

1. Each of these technologies (I.e. 3G, EDGE, etc) should be regarded as a “remote access” capability and all security standards relevant to remote access found in this document are applicable.

6.5 Security Training

NENA recognizes that security awareness training is critical to any organization’s security strategy and security operations. People are in many cases the last line of defense against many threats such as malicious code, disgruntled employees, and malicious third parties. Therefore, people need to be educated on what the organization considers appropriate security-conscious behavior, the applicable security policies implemented at their organization and what security best practices they need to incorporate in their daily business activities. All Public Safety employees shall annually complete security awareness training as established by each Public Safety Organization.

Additionally, entities responsible for system and security administration (including those contracted to do such tasks) shall employ individuals who have received current security training on their assigned system(s). It is the right of the 9-1-1 Call Center or similar agency to specify that a contracted agency hold specific or certain certifications to prove compliance with this requirement.

6.6 Suspicious Activity

Any suspicious or unusual activity, which may indicate an attempt to breach the integrity of Public Safety’s networks and systems, shall be reported immediately to an established Security Point of Contact / Team or equivalent. Any, and all, actual, attempted, and/or suspected misuse of Public Safety assets shall be reported immediately to the appropriate organizations.

6.7 General guidelines for design, development, administration, and use of any computer resource, network, system or application

Design, development, administration, and use of any computer resource, network, system, or application should always enable compliance with all security policy and requirements applicable to its intended use. Incorporating security into new products, services, systems, and networks before they are deployed shall be a priority. Security policy and requirements, and/or risk assessments should be a consideration in any development or product realization process. A security assessment of the controls and procedures should be conducted and documented before deployment to certify the compliance with security policy. This document should be retained as evidence for any future audit.

7 Safeguarding Information Assets

7.1 Identification and Authentication

Identification is the process by which one entity recognizes another entity, e.g., user, system or process.

Authentication is the provision of assurance of the claimed identity of an entity (e.g., individual user, machine, software component, etc.) The result may be Pass or Fail. The level of certainty with which the entity can be linked to the claimed identity will vary according to the authentication method used and operating practices.

In electronic information systems, authentication systems are hardware, software, or procedural mechanisms that enable a user to obtain access to network and / or computing resources.

Typically, a user identifies him or herself to the system by entering a unique User ID and password in response to a prompt. However, the authentication credential may take several forms, including passwords, digital certificates, or other shared-secret information (a combination of a token or smartcard used with a Personal Identification Number (PIN), also known as a Personal Identifier (PID).

7.1.1 Unique Identification and Authentication

All computer resources, systems, applications, and networks, which process Public Safety data, or data of others that Public Safety is obligated to protect, shall positively and uniquely identify and authenticate individual users prior to granting access. Any credentials used to identify and authenticate users or systems accessing computing or networking resources shall be assigned to individuals and not shared with anyone else, including work associates and managers.

7.1.2 User Access Management

The administration of user or entity access and accounts is a major component of security administration. The following outlines the minimum guidelines for processes such as assigning new entity accounts, resetting passwords, establishing resource access, and removing inactive accounts.

Requests for establishment of new entity accounts, User IDs and file and resource authorization shall be made through a process that can be documented and audited.

The request shall be approved by the authorized representative of the agency.

Personnel performing entity or security administration functions shall be responsible for ensuring that only approved entities are granted use and access to Public Safety's information resources. This requires that the identity of the requestor and of the approver, if required, be validated. This includes requests for password/PIN resets.

7.1.2.1 Changing Access

When a user changes job assignment, including promotion, demotion or termination:

1. The user's manager shall review the users access needs and notify all responsible administrators/help desks of job assignment changes within 24 hours.
2. Administrators or help desks shall delete or disable the IDs, or modify command and data access permissions of users within 24 hours of notification. Where access is no longer required the User ID shall be disabled and ultimately deleted when all use of the account is complete.

7.1.2.2 Disabling or Deleting Access

User IDs that have had no activity for 90 days should be reviewed with the approving manager for possible removal or deactivation. If the manager confirms that it is no longer required the User ID shall be deleted, otherwise it should be disabled. If feasible, system administration personnel should be informed of the need to remove an Entity's access to Public Safety information resources as far in advance of the need to remove the access as possible.

7.1.3 System to System Access

System to system access shall never mask individual accountability for transactions.

In any method of system to system data transfer, the source system shall first be authenticated before each transfer session. In the case of push technology, the destination shall be authenticated by the source. If the transfer method uses a continuous connection, authentication shall be performed at the initial connection.

Each system, application and machine shall have an identification and authentication mechanism built into the access path. One system/application/machine may perform security functions and controls for another system/application/machine dependent on the security relationship of the entities. The security services relationship shall be documented and approved in writing by the management of the interfacing systems/applications/services, and shall include a description of the security functions one entity is responsible for performing for the other.

7.1.4 Unsuccessful Login Attempts

A failed login attempt shall not identify the reason for the failure to the user, only that the login was incorrect, so as not to aid in subsequent unauthorized attempts to guess the right combination.

System login procedures shall be designed and implemented with a mechanism that will prevent the use of repeated login attempts to guess or otherwise determine a valid login identification and authentication combination. Systems shall lock the user out after no more than 5 failed login attempts.

7.1.5 Default Credentials and Control of Authentication Credentials

Null and factory default credentials shall be changed whenever installing new equipment or software. This includes all operating systems, applications and network infrastructure devices.

Authentication credentials shall not be visibly displayed when entered on computer screens, and when stored on computers, they shall be encrypted. When in written form, they shall be kept under lock and key and kept separated from associated User IDs and/or application names or devices.

Where two-factor authentication is used, e.g., SecurID + PIN, or Certificate + Passphrase, the two authentication factors shall not be stored in such a manner that a single event could compromise both factors.

Temporary credentials (which are credentials that are assigned by the Administrator, either when the account is initially created, or subsequently when a reset or reactivation is required) associated with User IDs shall require the user to change them at the first login. Where the technology permits temporary credentials shall be disabled if not changed within 30 days. If a credential does become, or is suspected of being, compromised, it shall be changed immediately.

7.1.5.1 Passwords

User Accounts and Passwords are common and effective mechanisms to control access to systems. It is important to not only require that all accounts used to access systems have passwords but that the passwords follow specific guidelines to maximize their success.

1. All User Accounts shall require a password
2. Password shall be adhere to the requirements listed in Table below:

Password Requirements

Option	Explanation	Required Minimum Value
Passwords must meet complexity requirements	Passwords are not based on the user's account name. Contains characters from three of the following four categories: • Uppercase alphabet characters (A–Z) • Lowercase alphabet characters (a–z) • Arabic numerals (0–9) • Non-alphanumeric characters (for example, !$#,%)	Enabled
Minimum password length	The setting determines the minimum number of characters that a user's password must contain. It is recommended that you change this setting from the default value of 0.	8
Minimum password age	This setting determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. A value of a few days discourages rapid password recycling while still permitting users to change their own passwords if desired. Note that setting this parameter to a value higher than the maximum password age forces users to call the IT department to change their passwords, which increases costs to the organization	3
Maximum password age	This setting determines the period of time (in days) that a password can be used before the system requires the user to change it. The best defense against impersonation is to require that users change their passwords regularly. This reduces the amount of time available for attackers to crack unknown passwords, and it periodically invalidates any password that has been stolen by other means.	60 (30 is recommended)

Enforce password history	This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be re-used. It also rejects new passwords that are too similar to previous passwords. This feature prevents users from circumventing password lifetime restrictions by reusing their old password. The default value is 1. Most IT departments choose a value greater than 10.	10

3. Where feasible, authentication schemes shall provide for password exchange in a format that cannot be captured and reused/replayed by unauthorized users to gain authenticated access, e.g., random password generating tokens or one-way encryption (also known as hashing) algorithms.

4. Passwords should not be hard coded into automatic login sequences, scripts, source code and batch files, etc, unless required by business need and then only if protected by security software and/or physical locks on the workstation, and passwords are encrypted.

5. Temporary passwords may be used when creating new accounts or resetting passwords, however, temporary passwords shall be required to be changed upon initial login.

The following additional password **guidelines** are provided to assist in educating users on how to create passwords:

- Password construction should be complex enough to avoid use of passwords that are easily guessed, or otherwise left vulnerable to cracking or attack. Names, dictionary words, or combinations of words shall not be used; nor shall they contain substitutions of numbers for letters, e.g., s3cur1ty. Repeating numbers or sequential numbers shall also not be used
- Passwords should not contain sequences of three (3) or more characters from the user's login ID or the system name.
- Passwords should not contain sequences of three (3) or more characters from previous chosen or given passwords.
- Passwords should not contain a sequence of two (2) or more characters more than once, e.g., a12x12.
- Passwords used to access Public Safety systems and resources should not be used on any external systems, e.g., Home PC's, Internet sites, shared public systems.

7.1.5.2 Passphrases

Passphrases are generally more secure than traditional passwords and should be used whenever possible. A Passphrase is simply a sequence of words or phrases used in place of a traditional password" to access a system.

Passphrases, when used, shall comply with the following minimum requirements:

1. Should be at least fifteen (15) characters in length.
2. Shall not use repeating words, or sequential characters or numbers.
3. Alpha, numeric and special characters may all be used.
4. Passphrases are case sensitive.

Where automatically set or set by administrator, the initial passphrase shall be randomly generated and securely distributed. First-time users may create their own passphrase after authenticating.

Users shall have the capability of changing their own passphrase online. The old passphrase shall be correctly entered before a change is allowed. A lost or forgotten passphrase can be reset only after verifying the identity of the user (or process owner) requesting a reset.

For a general System User, passphrases shall automatically expire every 180 days or less. Systems shall notify users at expiration time and allow the user to update the passphrase.

When a passphrase is changed, the old passphrase shall not be reused until either:

1. at least four (4) other passphrases have been used, or
2. at least 4 months have passed.

By default, systems shall not display the passphrase in clear text as the user enters it.

Passphrases shall not be stored in script files or function keys.

Passphrases shall always be encrypted for transmission

7.1.5.3 Digital Certificates

Where digital certificates are used for authentication, a revocation process shall exist in case of their compromise.

Digital Certificates that are expired or invalid shall not be trusted.

Owners of systems using digital certificates shall keep their certificates up to date.

Cryptographic implementations should use standard implementations of security applications, protocols, and format, e.g. S/MIME, SSL, SSH, IPSec, X.509 digital certificates. These implementations should be purchased from reputable vendors and should not be developed in-house unless properly trained staff is employed.

All employees shall protect and safeguard any encryption keys for which they are responsible. Private encryption keys shall not be shared with others except when applicable or appropriate authorities demand that the key be surrendered (i.e. Termination, Promotion, Investigation, etc). While public encryption keys are shared freely, access to the key shall be on a read only basis. Access to digital certificates shall also be on a read only basis.

A test of the validity of a digital certificate shall include the following:

1. The Certificate Authority (CA) signature on the certificate shall be validated
2. The date the certificate is being used shall be within the validity period for the certificate
3. The Certificate Revocation List (CRL) for the certificates of that type shall be checked to ensure that the certificate has not been revoked
4. The identity represented by the certificate — The "distinguished name" is valid (distinguished name refers to the location in the x.500 database where the object in question exists)

A process shall exist in which the current validity of a certificate can be checked and a certificate can be revoked.

Key holders shall initiate key revocation when they believe access to their keys has been compromised.

7.2 Access Control

7.2.1 Least Privilege

All access to computer resources shall be restricted to only the commands, data and systems necessary to perform authorized functions.

1. All data shall have appropriate minimum access privileges, e.g., read, write, modify, as defined by the owner of the data, and shall be maintained in compliance with local laws (some countries have very restrictive laws regarding access to employee information).
2. Access to data shall be restricted to only those individuals and groups with a business need, and subject to the data's classification. Unrestricted/global access should be avoided whenever possible and shall only be used where specifically appropriate and with the data owner's approval.
   a. An annual review of all resources, e.g., files or directories, to which access is not restricted, i.e., have universal or public access shall be performed and the resource owners shall be notified of the results.
   b. Common privileges can be assigned to a group of users, but membership to the group shall be restricted to only persons actually performing the given functions. For example, when responsibilities are divided on a geographic basis, the group memberships shall reflect that, i.e., different groups for different geographic regions.

3. All unnecessary services and network services shall be disabled. Any application service which lets the user escape to a shell, provide access to critical system files, or maps/promotes IDs to privileged user levels, shall be disabled.
   a. An annual review for compliance, which shall be documented including findings, shall be performed. Any findings shall be closed or risk managed.
4. Administrators shall ensure that system access controls, e.g., filters that restrict access from only authorized source systems, are used where they exist and shall only contain necessary system authorizations.
   a. System administrators shall perform an annual review for compliance, which shall be documented including findings. Any findings shall be closed or risk managed.
5. When not performing specific Administrative Tasks, System Administrators shall use an account with “non-privileged” rights. When Administrative Tasks are necessary, Administrators shall login in using their Administrative account to perform tasks then log back out. If supported by the system, features like “runas” or “superuser” should be utilized whenever possible.
6. Using a shared generic Administrator accounts (i.e. the Default Administrator account) shall not be used except during initial installation or under disaster recovery scenarios. Individuals who require Administrative access shall be assigned unique Administrative accounts where operating systems permit. Please note, an operating system that doesn’t support unique Administrative Access should be viewed as a significant security threat and should be avoided if at all possible. Entities are encouraged to prevent inclusion of such systems onto NG9-1-1 networks unless the mission absolutely dictates it.

7.2.2 Warning Messages

A formal statement of resource intent, i.e., a warning notice, shall be made visible to all those who access Public Safety computer resources and private internal networks. "Welcome" messages, which could be misinterpreted as extending an invitation to unauthorized users, shall not be used.

The login Warning notice shall be issued during the logon sequence (either directly before or after the authentication, preferably before, but it shall be displayed before any substantive data).

All personal computers, workstations and laptops shall display the notice at boot up.

The Warning message shall remain displayed until positive action by the user is taken to acknowledge the message.

The following is an example of a Warning Notice:

Warning Notice

This system is restricted solely to Public Safety authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by Public Safety. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, Public Safety may provide the evidence of such activity to law enforcement officials. All users shall comply with Public Safety policies regarding the protection of information assets.

7.2.3 Access Control Measures

Access control measures shall be utilized by all computer resources, systems, applications and networks at all times to restrict access to sensitive information or system/network processors to authorized personnel only. Such measures could include the use of system configuration, file system permissions, system rights or access control software, etc

Where possible access control shall be accomplished with "role-based" privileges that assign users to roles and grant access to members of a role rather than to individuals.

7.2.4 Sensitive File/Resource Access Permissions

Non-privileged users shall not have read/write access to system files or resources such as protected memory, critical devices, executable programs, network configuration data, application file systems, etc. Only users who have administrative responsibilities, e.g., administrators and their designated backups, may be assigned passwords to access and modify these sensitive files/resources.

7.2.5 Rights & Permissions

In order to properly protect a network and, ensure that proper access is given only to those who need it, user rights and permissions must be understood. It is important to understand the difference between a right and permission.

- A right is a property that is assignable to a user or a group, which will either allow or deny them the ability to perform an action. A good example of this is the ability to install a printer on a computer; this is an allowable right that can be assigned.
- A permission, on the other hand, grants or denies access to an object or resource. This would allow a basic user to see only their files while allowing management to see all of the files.

It is also important while implementing these rights and permissions to determine if there are any specific restrictions that need to be enforced, i.e., Law enforcement data can't be shared with Fire/EMS and patient records must be kept confidential consistent with the classification of the data.

The following requirements are provided:

- Access to Files/Folders shall be limited only to those who actually need access
- Home directories, home shares, etc., associated with a User ID shall initially not be readable or write-able by anyone other than the owner of that User ID

- Rights shall be assigned only to those who actually need them and are documented as needing them
- Permissions shall always be configured in accordance with the classification of the data
- Groups should be used whenever possible to simplify administration
- Adhere to the policy of least privileged use, meaning if a basic user can perform all of the tasks necessary, don't grant administrator access to them.
- Rename built in Administrator accounts
- Disable Anonymous or Guest accounts as these typically can be exploited.
- Periodically run audits against users to determine what their effective rights and permissions are. If a user is a member of several security groups it is possible for that user to have elevated privileges that were not intentional.

7.2.6 Separation of Production from Non-Production Systems

For purposes of this document, Production Systems include Training Systems which are intended to become live production systems and therefore shall meet the same criteria as production systems. Production systems (including networking components) shall be separated from non-production systems to ensure the integrity of production data. Physical separation is preferred, but at minimum, logical separation is recommended. If physical separation cannot be achieved then Non-Production Systems must adhere to the same security levels of Production Systems.

Production systems shall not contain any software development tools, such as software compilers and libraries, except where essential for the application. Such tools may be installed during software upgrades or for the installation of new software packages, or for troubleshooting purposes, but shall be removed immediately after their use. Where such tools are essential for production operation, they shall be made inaccessible to users, e.g., placing PERL interpreters in separate directories, not accessible from the web.

Non-production data shall not be transmitted or moved into a production environment without going through proper change control process and receiving authorization, i.e., system/process owner.

Developers shall not be system administrators for production systems for which they have responsibility, i.e., segregation of duties shall exist; except for small stand-alone systems.

Development personnel with a legitimate business need shall only be given access to production systems and data in accordance with, one (or more) of:

1. The system's outage/recovery procedures, e.g., disaster recovery plan.
2. Temporary (time-bound) read-write access when approved via change control.
3. Permanent read-only access.

Any software and/or data changes initiated as a consequence of an outage/recovery procedures or temporary write access shall be documented and retained until it is determined that the production system and data were not corrupted. Production data shall not be copied off a production system without the service owner's authorization and shall be protected to an equivalent, or greater level.

7.2.7 Screensavers and Inactive Sessions

All devices capable of enforcing a password protected screensaver or a keyboard lock shall do so with the inactivity timeout set to 15 minutes or less, except:

1. When superseded by local Public Safety policy.
2. Users in a customer facing role, such as sales representatives making sales presentations, may have the automated screensaver temporarily disabled so long as the following conditions are met:
    a. The automated screensaver shall not be deactivated for any longer than justified and not for a period greater than four (4) hours.
    b. While the automated screensaver is deactivated the screensaver shall be manually activated whenever the device is to be left unattended, even for a brief period of time.
3. Devices that are dedicated to displaying messages/information to a number of people, for example, in a reception area or in an operations center, may have their screensaver disabled so long as the following conditions are met:
    a. Access (physically and logically) to the device, including its keyboard and User IDs, is controlled in accordance with all applicable physical and logical security requirements.
    b. Visibility of the display is restricted to only individuals authorized to see the data that will be displayed.

Devices not capable of enforcing a password protected screensaver or a keyboard lock, such as dumb terminals, shall have at least one of the following:

4. Access (physically and/or logically) to the device, including its keyboard and User IDs, controlled in accordance with all applicable physical and logical security requirements.
5. The console is configured to automatically logout after 15 minutes of inactivity (This is not to terminate running commands).
6. Have session inactivity timeouts set for 15 minutes.
7. Users logout when console is left unattended if automatic inactivity logout is not supported

NOTE: The time taken by network components to allow firmware or software updates to complete is not to be considered a period of inactivity.

Hence, personal computers utilizing the operating system's screensaver typically does not need to have their applications include inactivity logic.

7.2.8 Future Communication Services

Public Safety is a mission critical production environment. Security assessments shall be conducted for any new form of communication that wants to be added or linked to a NG9-1-1 environment. Only after sufficient security control is in place can such new forms of communication can become connected. The following sections provide best practices and recommendations for securing such new forms of communications.

7.2.8.1 Business and Security Risks

Before the traditional security enforcement and deployment of new forms of communication, a risk assessment should take place, the followings shall be considered by the public safety community as business risks:

1. the resource availability impact,
2. business justification or importance of the service or data to use a specific communication method (the utility of the service compared to the security risk),
3. false-positive rate (e.g., the possibility this new form of communication can generate false alarms while there are no security vulnerabilities),
4. false-negative rate (e.g., the potential of unknown new vulnerability is introduced by this new technology while the vulnerabilities are undetected),
5. legal status (e.g., liability, contract language, recording as evidence, authority to access information, privacy protections),
6. volume (normal, bandwidth, latency, diversity/redundancy induced denial-of-service, etc).

Business risk (of the public safety community) acceptance shall not be the charter of the security function.

7.2.8.2 Communication Partners and Scope

Beyond technology, the users using new forms of communication can be confined by their realms (for the purpose of this document a realm is a network or service with specific security characteristics). One realm may or may not be allowed to communicate to other realms. More importantly, some realms may not be trustworthy. For example, a known email service provider where 97% of the emails originated/relayed from that realm are spam emails, unchecked email senders, or virus-infected.

The scope definition may be controllable by creating a communication partners white-list. Be aware such a list may also be a “moving target”. Selection of a reputable, experienced service provider is highly recommended because a seasoned service provider usually knows how to keep up with the most recent “security climate”. A good service provider may even declare an emergency to temporarily block the gateway to its peering partners to confine the risks when it detects an outbreak of security events pertinent to its service.

7.2.8.3 Information Delivery Service Demarcation

The new forms of the communication methods may be performed by one or multiple-cascaded[1] service providers. Some service providers may even perform the format conversion function as a gateway in between the new format and the legacy format.

Example 1, an IP-enabled Telecommunications Device for the Deaf (TDD) service provider may have one listener side on the IP space while its output is the standard legacy TDD circuit to the TDM world. In this example, the demarcation from NG9-1-1 EntityNG9-1-1 Entity point of view is still the traditional TDM switch, not anything related to TDD-IP.

Example 2, a VoIP Gateway "Wholesale" Clearing House is performing a VoIP gateway function[2] for the entire NG9-1-1 EntityNG9-1-1 Entity communication, i.e., put the shareable functionalities/new technology in the cloud, then feed and serve individual NG9-1-1 Entity as a "virtual facility" using the traditional/legacy communication method.

These may be the potential new service provider models and their demarcation and associated roles/responsibilities/SLA will be different than NG9-1-1 Entity's own. On the other hand, if such function is performed within the NG9-1-1 Entity (by NG9-1-1 Entity itself or by a service provider within), the responsibilities will "move", since the demarcation might have moved.

7.2.8.3.1 Client Software Add-ons ("Plug-ins") Security Risk

Many add-on or plug-in features are not needed and occasionally become a security risk. For example, browsers may allow a new "software plug-in" (i.e. Flash, Shockwave, Java, etc) to be installed without its true intent being identified (a worm, a key-logger, a Trojan to steal database content). Another example is a piece of software may allow a file being transferred into or out of the NG9-1-1 Entity environment without any form of approval. The arbitrary installation of plug-ins can potentially cause security risks to the NG9-1-1 Entity.

Therefore, all client software installed in NG9-1-1 environment shall be approved, inventoried and audited for compliance, including appropriate version. Client software shall not be configured to auto accept the software add-on or plug-ins.

Compliance checks shall occur in concert with the audit schedules defined in section 11 of this document.

All new add-on software or plug-ins shall be tested before installation.

It is noted that many tools exist that can be used by NG9-1-1 entities to assist in the automation and policy enforcement of software add-ons, etc.

[1] intermediary service providers in the delivery chain

[2] In one of the NENA proposal, it seems to be the direction they are advocating.

7.2.8.4 Peer-to-Peer Networking

Peer-to-Peer (P2P) Networking has become quite popular since it leaves the “central server and the potential for its control” out of the picture. For example, in a music-sharing application, the central server just serves as the indexing function, i.e., answer one client’s question: “who has the music collection by the name Happy Birthday”, once the answer is given, the central server is out of the picture (the P2P service provider attempts to avoid legal liability/lawsuit especially from content/title holders.) Then the File Sharing part of client software kicks in using UDP to talk directly to another computer who claims it has that piece of music. P2P’s software client is well-known to be infected with Trojans and its “business need” list is nil.

The P2P solutions that exist today are unsuitable for use in NG9-1-1 environment. This may change but until such time as reasonable IT Security standards for P2P are adopted, P2P shall not allowed in the NG9-1-1 environment.

7.2.8.5 Hybrid Communication Method: VoIP

NG9-1-1 entities might already run one form of VoIP (i.e. County VoIP system). Security becomes an issue when another VoIP realm needs to communicate with another VoIP system within the NG9-1-1 Entity. From security point of view, this becomes the question of how to securely interface with other realms.

The NG9-1-1 Entity should not connect its own system with others (i.e. connect the NG9-1-1 VoIP system with the County’s VoIP realm) without securing the connectivity.

7.2.8.6 Telecommunications Device for the Deaf (TDD)

The security of legacy TDD devices and communication methods is outside the scope of this document.

Future advancements for emergency services communication in the hearing and speech impaired community may require security requirements to be established at a later date.

7.3 Confidentiality

7.3.1 Disclosure of Information

As noted in this document, all information shall be classified and handled appropriately. However, some information captured by the NG9-1-1 Entity may fall into the public domain and be either discoverable or otherwise requested by the general public or media. Data falling into this category shall be clearly identified and specific guidelines written and followed to document what data is released, when and to whom. Further, these guidelines shall capture any specific release requirements for data such as video, names, call content, message text or other personal content. Where such data is intermingled with other data of differing classification, consideration shall be given to replicating the public domain data into a separate data store.

7.3.2 Email Security

Future NG9-1-1 deployment models may leverage or utilize email based emergency communication systems. It is important to understand that email based emergency notification systems are viewed by this document as different from a NG9-1-1 Entity's internal email system.

The use of email in any scenario should be done with caution. It is recommended that internal NG9-1-1 Entity mail not be made available on a 911 call-taking position workstation but rather on a separate system. However, email based emergency communication systems shall be allowed with appropriate security mechanisms. NENA has not defined email security standards in this release of the document, but may do so at a later date. In lieu of standards NG9-1-1 entities are encouraged to follow best practices such as those offered by the National Institute for Standards and Technology (NIST)

Additionally, personnel who use electronic mail systems to send NG9-1-1 Sensitive information shall implement appropriate security controls to assist them in protecting incoming and outgoing messages. The originator of an email message containing Proprietary information should ensure that:

- The message is clearly marked to reflect its proprietary classification.
- The email ID to which the information is being sent is correct.
- The recipient of the email message understands the safeguards associated with the proprietary marking. The originator of the email message may have to explain the safeguards to the recipient of the email message in advance.
- If printed, the email message shall be protected according to the rules associated with its proprietary marking.
- The proprietary information is encrypted in accordance with NG9-1-1 Entity requirements.
- Internal mail shall not be automatically forwarded out the internal network, such as via the Internet, to any other mail system.
- NG9-1-1 EntityNG9-1-1 Entity employees and contractors shall only use a NG9-1-1 EntityNG9-1-1 Entity domain email address to conduct business unless otherwise obligated to do so through a formal contractual document.
- NG9-1-1 EntityNG9-1-1 Entity database systems which are used to define the contact details for personnel performing work on behalf of NG9-1-1 EntityNG9-1-1 Entity shall only contain email addresses within NG9-1-1 EntityNG9-1-1 Entity domain unless covered by contract.

7.3.2.1 Text Messaging

Individual messaging services, e.g., SMS, need to be evaluated to ensure the service characteristics, service grade, contract language, and security posture can meet NG9-1-1 Entity production and security requirements.

7.3.2.2 Video-Clip Multimedia Messaging

In mobile phone services, there is a multimedia messaging service (e.g., MMS) which allows “video-clips” being captured by the mobile device to be sent to the recipients, similar to SMS message delivery scheme except that the content is enriched. The source of the multimedia material is the cellular phone’s own camera but due to technological advancements such technology could be falsified or obtained from video sources e.g., Internet posted, PC edited “video productions, etc. For such service to be considered as an acceptable (authenticity, secured, and valid) data feed for NG9-1-1 Entity, it needs to be evaluated to ensure the service characteristics, service grade, contract language, and security posture can meet NG9-1-1 Entity production and security requirements. These can be independent efforts and are out of scope of this document and/or may be addressed in a future release.

7.3.3 Encryption and PKI

7.3.3.1 Encryption Algorithms

Cryptographic implementations shall use industry standard cryptographic algorithms and standard modes of operations. It is recommended that the algorithm certified by the US National Institute of Standards and Technology’s (NIST) FIPS 140-1 certification, currently AES, be used. More information on current US federal encryption standards and modes of operation is available from the NIST Computer Security Resource Center.

Where there are no applicable US federal standards for specific encryption functions, e.g. public key cryptography, message digests, commercial algorithms may be used, e.g. RSA, Diffie-Hellman, RC4, and SHA-1. Implementations and modes shall follow best commercial practices, e.g. Public Key Cryptography Standards. Implementations and modes shall use the strongest available product. More information is available at: http://www.rsasecurity.com/rsalabs/pkcs/index.html.

The use of any encryption algorithm or device shall also comply with the laws of the United States and those of any country in which there are plans to use data encryption.

7.3.3.2 Key Lifecycle Management

The current state-of-the-art in information security relies upon Public Key Cryptography. Simply put, Public Key Cryptography uses pairs of keys to lock and unlock data. When Public Key Cryptography is used to securely send data, one key, the private key, can only unlock the data, while another key, the public key can only encrypt data. This means that the public key can be freely distributed.

If Bob wants to securely send data to Mary, he can look up Mary’s public key, and use it to encrypt the data. Once this is done, only Mary’s private key can decrypt the data. As long as the private key is kept secure, Public Key Cryptography is very safe. Since the private key is never exchanged, keeping the private key safe is easily done. There is no need to secure the public key since it cannot be used for decryption. This makes it easy to distribute the public key to those who want to securely send information. To efficiently implement Public Key Cryptography, a Public Key Infrastructure (PKI) is used to manage and distribute the public keys.

For both Symmetric Key and Asymmetric Key cryptography, management techniques shall exist to manage the lifecycle of the cryptographic keys, such as creation, distribution, validation, update, storage, usage, and expiration.

All personnel shall protect and safeguard any encryption keys for which they are responsible. Private encryption keys shall not be shared with others except when NG9-1-1 Entity demands that the key be surrendered. While public encryption keys are shared freely, access to the key shall be on a read only basis. Access to digital certificates shall also be on a read only basis.

Encryption devices and any server used for storage of encryption keys shall be protected from unauthorized access.

Key generation shall be performed using commercial tools that comply with x.509 standards and produce x.509 compliant keys. Keys shall not be generated or derived from predictable functions or values, e.g. values considered predictable include user identity information, time of day, stored/transmitted data.

Symmetric keys shall be at least 112 bits in length.

Asymmetric keys shall be at least 1024 bits in length. However, this shall be increased to 2048 bits where feasible.

Keys, whether symmetric, secret keys or PKI based key-pairs, shall be expired and new keys generated in accordance with industry acceptable practices. Decrypting keys may be revoked at any time if a responsible employee or NG9-1-1 Entity believes the key has been compromised, or if the NG9-1-1 Entity no longer employs the person assigned those keys.

Keys shall only be distributed to appropriate recipients through secure channels. Keys used for encrypting stored data shall be safeguarded so that authorized persons can recover them at any time in order to recover NG9-1-1 Entity data or information

7.3.3.3 Public Key Infrastructure

The use of a Public Key Infrastructure (PKI) is encouraged to support applications (e.g. secure email and SSH) that need encryption, authentication, and signing functions.

Any PKI that is used or implemented shall have a documented Certificate Practice Statement (CPS) that defines how security is provided for the infrastructure, the registration processes, relative strength of the system, and legitimate uses of the infrastructure. Hence, the CPS ensures that the PKI provides appropriate services and protections necessary to meet the needs.

A PKI shall implement a registration process that verifies the identity of a digital certificate requestor using an acceptable form of identification prior to the CA creating a digital certificate that binds the requestor's identity to the public key provided. The choice of acceptable form of identification shall be based upon the level of trust required within the PKI. If a high level of trust is required, then a possible form of identification may be a Photo ID, e.g. passport. The choice of process shall also consider the strength of the private key protection for certificate holders.

A process shall exist in which the current validity of a certificate can be checked and a certificate can be revoked.

Key holders shall initiate key revocation when they believe access to their keys has been compromised.

7.4 Integrity

7.4.1 Obtaining Files or Software

All files and software shall be obtained from trusted sources, and shall be scanned for viruses and malicious code. Any binary or executable files obtained from un-trusted sources, shall be verified to be free of logic bombs or other malicious code before being used.

Freeware, Shareware & Open Source software shall be obtained from a reputable source, e.g. Public Software Library (PSL). If obtained from non-trusted sources such as Internet web sites, it may not be used on NG9-1-1 Entity computers unless authorized by management.

7.4.2 Maintaining Accurate Time Reference

Time synchronization shall be in accordance with the NENA 04-002 NG9-1-1 Entity Master Clock standard.

7.4.3 Computer Viruses and Malicious Code

Any device used to conduct business that is capable of running anti-virus (sometimes now called anti-malware) software shall have that software installed, running and up to date to protect from virus infection. The essential trustworthiness of the software used to conduct NG9-1-1 Entity business shall be maintained, i.e., kept free of viruses and other malicious programs.

Personnel, including all contractors with current service agreements, shall:

1. Install and maintain the latest version (including engine) of the licensed anti-virus software.
2. Update servers and workstations, including personally owned equipment used for business, with the latest version when made available.
3. Antivirus software shall be current with the latest available and applicable virus definition files
4. Scan all files when opened and/or executed (including files on network shares).
5. Scan all files on all local drives at least once a week.
6. Scan all files, attachments and software received via email and/or downloaded from web sites before opening and/or executing.
7. Scan all removable media and software (including new workstations equipped with pre-loaded software) before opening and/or executing.

8. Scan all removable media and software before opening and/or executing if it has not been kept secure within your control.

Additionally, server administrators shall scan all files made available as network shares at least once a week.

7.4.4 System Changes

Any changes to computer system hardware and operating system software shall adhere to the following:

1. Formal documented procedures shall exist and be followed.
2. Appropriate level of authorization shall be required and obtained prior to change(s).
3. The Administrator shall control software changes that affect the operation of an application, operating system, or utilities. This includes updates and upgrades that could affect user response, machine performance or operations, security, or system availability.
4. A detailed audit trail of all modification to network hardware and software shall be created, retained and reviewed at least annually.
5. Records of all system/application changes should be retained for a minimum of three years and in no cases less than 1 year or the last major upgrade whichever is longer.
6. System Controls shall indentify accountability for all program changes to a specific programmer, and approving manager.
7. Exception reporting procedures shall be built into system software to detect computer, program, communications, and operations failures. Error checking and validation controls shall be in place, e.g., checksum monitoring, to validate the integrity of the data.
8. Ensure current backups provide the capability to recover in the event of system problems created by the changes.
9. In cases where system administration or maintenance is outsourced, all records kept by such agencies shall be available to the NG9-1-1 Entities to review.

7.4.5 System Patching

Vendors and security organizations issue either alerts or advisories relating to security flaws that allow unauthorized access to systems or data, to bypass access controls, or gain unauthorized privileged authority as they are discovered in operating systems and other software. All available and applicable vendor-provided patches that address critical security vulnerabilities and have been approved by management for use shall be applied as quickly and prudently possible. Testing of patches is strongly encouraged.

NOTE: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of a NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode. Examples of alternative operation modes can be:

– route 911 traffic to an isolated and hardened NG9-1-1 Entity

– raise firewall to prevent further spreading of virus/worm

– re-direct calls to an administration work station

– exercise emergency restoration options

Procedures shall be instituted which verify and document that the business hardware and software are currently supported by the manufacturer or supplier such that advisories are issued and fixes are made available for any newly discovered security vulnerabilities.

Where possible, permanent fixes shall be used in preference to temporary fixes. However, where a temporary fix (work-a-round) is advised and a permanent fix is not available, the temporary fix shall be used within the prescribed timescale until a permanent fix becomes available.

A process shall be in place to ensure that all applicable permanent fixes are installed, and that temporary fixes cannot become disabled until the permanent fix has been installed.

All fixes (temporary or permanent) shall be tested prior to using them in a production environment. Testing shall also be done to ensure that no security vulnerabilities are introduced, e.g., unnecessary services or default User IDs re-enabled.

7.4.6 Server and Workstation Configuration

Servers, End-users workstations, desktops, or laptop PCs shall be hardened (i.e. unused services disabled, and no “local administration right” is given to the end-user, etc). Any exception shall go through the applicable approval process. NG9-1-1 entities should follow recognized best practices for Operating System hardening like the National Institute for Standards and Technology (NIST) guidelines or the ISO 27002 standards.

In a few cases, e.g., Business Continuity/Disaster Recovery during emergency evacuation, laptop PCs (e.g. call-taker position, CAD, MIS PCs) may be moved from one NG9-1-1 Entity to another NG9-1-1 Entity. During the transit, these machines’ configuration shall not be changed. Unless explicitly approved, these machines shall not be used/powered on during transit.

In this document, virtual office[3] workstation/PC arrangement, either using NG9-1-1 entity provided PC or personally owned PC, is not recommended due to the high sensitive nature and high reliability requirement of the NG9-1-1. However, if properly secured this model along with Virtualization may be a viable option as newer technologies to secure this information in this environment are developed and implemented.

7.5 Availability

There is often an extremely high cost associated with achieving 100% uptime availability. The realistic goal is to achieve ***near***-zero down time. It is at the discretion of each NG9-1-1 Entity to weigh cost and security against availability to achieve the desired balance and/or set the applicable level of targeted uptime.

Critical and non-critical services may have different availability levels. While some services are difficult to duplicate other services may be temporality augmented or reduced. For example, if the ALI linked CAD is not functional; a manual lookup method allows the equivalent. This is a slower method, but the service is still available. Another example would be if the ALI or map is not available, E911 service would be temporarily degraded to basic 9-1-1 service.

7.5.1 Security Impacts to Availability

Security functions are required to deter the intentional or unintentional attacks from an environment outside the NG9-1-1 Entity, from reaching into the NG9-1-1 Entity's inside perimeter causing damage and outage. Security measures shall be as transparent as possible and should not be an insurmountable burden in achieving high availability.

Redundant links, backup connection using on-demand dialing, or other arrangement can be chosen for increased link reliability.

From a security work function point of view, the two main security goals shall be:

1. Fulfill security tasks while maintaining the availability of the NG9-1-1 Entity.
2. Perform maintenance tasks while retaining supportability and administrative functions.

The security design shall make the environment serviceable and all possible failure scenarios shall have the corresponding actions pre-planned.

7.5.2 On-Site/Local High Availability

Building high availability in networks can be handled by multiple elements such as:

1. Redundant LAN switches

[3] E.g., working from home arrangement

2. Teamed[4] NICs in servers and mission-critical desktop computers
3. Redundant servers
4. High availability or redundant firewalls
5. Redundant routers
6. Redundant WAN links
7. Out-of-band communication links
8. Redundant management LAN/WAN
9. Remote control board for servers
10. RAID arrays
11. Dual-CPU and/or other high-available server designs
12. Redundant premise wiring
13. Redundant HVAC

The goals shall be:

1. Any single point of failure is identified and the alternative strategy is planned and documented.
2. Distribute the down-time window, if possible. For example, if an approved security patch is about to be applied to a server farm, apply them in the proper order such that at minimum one server will still be in production while others are being patched/rebooted.
3. All equipment shall be managed and monitored such that if one of the high availability elements is already down, the status shall be made known to the NG9-1-1 Entity and the management entities. Authorization for expedited service and the associated costs should be considered.
4. Plans shall be thoroughly tested and documented. Annual drills shall be exercised and post-mortem analysis and action plans produced.

7.5.3 High Availability by Geographic Redundancy

Local high availability may not cover all failure scenarios and may not work all the time. It may be necessary for a back-up facility to temporarily assume work functions. This may be required for NG9-1-1 Entity functions, service provider functions or possibly both.

Geographic redundancy shall be pre-planned, be it a partner or mutual-support NG9-1-1 Entity, or a service provider’s alternate data center. The communication path shall be re-routed in an acceptable and pre-defined timeframe.

[4] NIC teaming is a technology offering two separate paths into the same server where only one IP address is known to the local area network.

The fail-over scenarios shall cover trigger-driven events (e.g., threshold crossing) as well as pre-scheduled events (maintenance downtime). Fail-back criteria shall also be defined such that a smooth transition back to normal production arrangements can take place.

7.5.4 Backup/Restore and System Recovery to a Secure Condition

Operationally, the NG9-1-1 Entity and its suppliers/service providers shall have a strategy to deal with system failures. Backup storage media may be magnetic media, optical media, etc. Note that the actual storage may or may not reside in the same physical location as the operational systems. A backup and rotation schedule should be established. Backup media should be securely stored. If restoration is needed, sufficient care shall be taken such that during restoration, sensitive information will not be leaked out or privileged information (e.g., root or Administrator password) will not be disclosed. A copy of the routine full backup media shall be sent to a secure offsite location for archiving and Disaster Recovery (DR) purposes.

7.5.5 Business Continuity and Disaster Recovery

The high availability design shall cover the normal course of a NG9-1-1 Entity's production scenarios based on reasonable time-and-cost assumptions. There are other scenarios which are beyond normal situations, (e.g., wars, major catastrophic, etc). Under such situations, Business Continuity and Disaster Recovery (BC/DR) mechanisms[5] may be invoked. BC/DR plans shall be created but this is beyond the scope of this security document.

However, NG9-1-1 Entities are reminded to take the entire network operating requirements into consideration when developing Business Continuity and Disaster Recovery plans. A worst case scenario should be assumed; you are not functioning and neither is anybody else in the immediate area. Recovery within 50 miles of your current location is highly unlikely. Plans should be made for a distant recovery site.

BC/DR drills shall be conducted periodically within a fixed interval to be defined by local policy and minimally on a per annual basis.

7.6 Audit and Accountability

Systems, including but not limited to applications and databases, shall have internal controls for logging, tracking and personal accountability.

7.6.1 Security Audit Logs

Systems, including but not limited to applications and databases, shall have a security event record (log) mechanism that is capable of providing information sufficient for after-the-fact investigation of loss, impropriety or other inappropriate activity. A system, or if necessary, a

[5] E.g., use alternate communication method such as Ham radio, WAAS radio, cellular phones, emergency broadcast system, etc.

group of interacting systems, shall have end-to-end logging capability sufficient to substantiate user accountability for all significant events within the system and among the interacting systems. A log collector product or process shall be used to periodically retrieve the data from the target systems and archive them outside of the original systems creating the log events.

All resources to which access is controlled including applications and operating systems shall have the capability of generating security audit logs.

All security logging mechanisms, e.g., UNIX® accounting, shall be active from system initialization. These mechanisms include any automatic routines necessary to maintain the activity records and cleanup programs to ensure the integrity of the security audit/logging systems.

7.6.2 Security Audit Log Review

Administrators shall develop and document a security audit log review plan to include:

1. the frequency for security audit log review based upon such criteria as: criticality of the system, business risk, cost, system classification, and
2. the minimum unusual activities to be reviewed for, these might include for example: multiple unsuccessful login attempts, user attempts to access files or resources outside their privilege level, network activity.

Where the security audit log review is automated, anomalies in the security audit log shall be alarmed.

7.6.3 Security Alarms

Administrators shall develop and document a security alarm plan to include:

1. the undesirable events such as potential security problems or suspicious activity for which security alarms shall be generated, e.g., high volumes of bad packet data, corrupted data, attacks, or information gathering attempts.
2. the threshold levels for these events. These shall be set so as to detect events that might impact the service, enabling action to be taken, while not resulting in an excessive number of false alarms.

At a minimum, security alarms shall be activated automatically by the following events:

3. Six (6) consecutive unsuccessful login attempts.
4. Successful modification of critical system or application files (as defined by the administrator).
5. Unsuccessful attempts to gain permissions or assume the identity of another user.

8 Physical Security Guidelines

All NG9-1-1 Entity information resources shall be kept physically secured and protected from theft, misappropriation, misuse, unauthorized access and damage.

8.1 Building and Physical Access Control

1. Doors with security mechanisms shall not be propped open.
2. Employees, suppliers, contractors and agents authorized to enter a controlled physical access area shall not allow unidentified, unauthorized or unknown persons to follow them through a controlled access area entrance.
3. Each person entering a controlled access facility shall follow the physical access control procedures in place for that facility.
4. Personnel shall be vigilant while inside the building and challenge and/or report unidentified persons including persons not displaying identification badges who have gained access.
5. When automated access control and logging devices are installed, personnel shall use them to record their entry and exit.

8.2 Authorized Physical Entry

8.2.1 Resident and Recurring Non-Resident Authorized Entry

All building residents and other persons authorized for recurring, unescorted entry into a NG9-1-1 Entity facility that houses information resources shall be permitted entry only in accordance with the following paragraphs.

Physical access control devices issued to an individual shall never be loaned to, or shared by, another person.

A person possessing an access control device shall never use that device to allow access to an unauthorized person.

8.2.1.1 Non-Employees

Non-employees who are to be issued NG9-1-1 Entity identification badges, building access cards, building keys, and/or any other form of recurring access that does not require approval at the time of access shall be sponsored by a NG9-1-1 Entity management person.

Appropriate local, state and federal laws and guidelines shall be followed for allowing non-employee access (i.e. CJIS Background Checks, etc).

8.2.1.2 Identification Badges

Identification badges containing a picture of the holder shall be issued to all residents of buildings containing information resources.

If the facility is guarded, the identification badge shall be displayed to the guard upon entry into the facility.

Identification badges shall be displayed by a person at all times while in a NG9-1-1 Entity facility and/or on NG9-1-1 Entity premises.

A person on NG9-1-1 Entity premises shall present his/her identification badge for examination and/or verification upon request. Failure to comply may result in removal from the facility and/or denial of further physical access to the facility.

Building residents and non-residents with recurring access authorization who do not have a valid identification badge in their possession shall be signed in and vouched for by an authorized building resident who possesses and displays a valid picture identification badge.

A temporary identification badge shall then be issued and the number of the badge recorded on the sign-in log along with the identity of the person vouching for the entry.

Possession of a temporary identification badge does not constitute permission to reenter a building. Identification, sign in and authorization procedures shall be followed.

A temporary badge shall be returned when the person leaves the building.

Lost or stolen identification badges and/or building access keys or cards shall be reported to the ENTITY that issued the badge, key or card.

8.2.2 Entry by Others

Persons holding any NG9-1-1 Entity picture identification badge shall display this badge at all times while in/on the site.

All those requiring non-recurring entry shall be signed in by a person who displays a valid NG9-1-1 Entity picture identification badge that authorizes that person entrance into the site. A temporary identification badge shall then be issued to the visitor and the number of the badge, the person's name, the date and the name of the person authorizing the access shall be recorded on a sign-in log.

The person shall display the temporary badge at all times while on NG9-1-1 Entity premises.

All temporary badges shall be returned when leaving the building and the log shall be noted accordingly.

All visitor temporary identification badges shall have the words "Escort Required" prominently displayed. Persons displaying temporary identification badges with the words "Escort Required" and who are not escorted shall be removed from the building.

Lost temporary identification badges shall be reported immediately to the ENTITY that issued the temporary badge and attempts shall be made to recover the temporary badge.

Possession of a temporary identification badge does not constitute permission to reenter the secured area for which the badge was issued. Identification, sign in and authorization procedures shall be followed.

8.3 Storage Media and Output

Data stored on removable media that is external to the system hardware such as diskettes, tapes, cartridges, USB memory devices, and Optical Media shall be safeguarded.

Personal storage devices (i.e. user owned USB thumb drives, etc) shall not be used.

Sensitive data shall be printed on an attended printer or one in a secured area. Distribution of the output shall be controlled. Printouts containing sensitive or critical information shall be kept in

All printouts containing classified information shall be protected.

When producing copies of printouts containing classified information, the originals and/or copies shall not be left unattended at the copier.

Storage media and output (e.g. CDs, tapes, diskettes, hard disk drives, printouts, memory chips, flash drives) shall be destroyed in such a manner that the contents cannot be recovered or recreated

NG9-1-1 Entity personnel shall ensure that re-used storage media is "clean", i.e., does not contain a residual of information from previous uses.

All media distributed outside NG9-1-1 Entity shall be new, or come directly from a recognized pool of "clean" media.

8.4 Mobile Devices

8.4.1 Security in the Work Area

All portable computing devices, including, but not limited to laptops, Personal Data Assistants (PDAs), data backup/storage devices, communications devices, testing devices, monitoring equipment and authentication devices, shall be kept physically secured as denoted below:

- When equipped with locks, portable computing devices shall be kept locked to prevent theft. Keys shall be stored in a secured location.
- Docking station style portable devices shall be locked in a secure location (i.e. File Cabinets, Safes or Desks) when not in use. Docking station style portable computing devices shall not be left unattended outside normal business hours even when in the docking station.
- Other portable devices shall be stored in a locked cabinet, drawer, or office (not just the building) when not in use.
- Extra security precautions shall be implemented in and around the receiving, staging, assembly and storage areas used for large deployments of portable computing devices.

8.4.2 Security Outside the Work Area

- Portable computing devices shall be secured when unattended (i.e. in hotel and meeting rooms). Use locking cables and/or other restraints whenever possible.
- Portable computing devices should also be concealed from view whenever possible when unattended.

- Computers shall not be left in view inside unattended vehicles.
- Vigilance shall be maintained in airport luggage inspection and transfer areas, hotel check in and check out areas, and other public areas.
- Devices shall not be left unprotected in conference rooms, etc.
- If possible, information resources using a power supply shall be connected to electrical outlets and communications connections that utilize surge protection.
- Devices shall not be exposed to extreme heat or cold.
- Whole disk encryption should be used whenever possible.

8.5 Environmental Controls

Information resources shall not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions shall also be taken to ensure that information resources cannot be affected by problems with utilities, such as water, sewer and/or steam lines that pass through the facility.

All information resources shall be protected from damage caused by spills, etc., from food or drinks.

At a minimum, all buildings housing significant NG9-1-1 Entity information resources shall have a documented fire plan, smoke and/or fire detection devices, sprinklers or other approved fire suppression systems as required by local code, and working fire extinguishers in easily accessible locations throughout the facility.

Information resources using an electrical power supply shall require UPS or surge protection as noted below:

If the information resource is critical to business operations, a UPS shall protect the information resource or the processing performed shall be duplicated or mirrored in a second location not generally subject to the same power outage.

All buildings containing critical information resources shall have protective physical measures in place. Physical access to other critical support facilities in the immediate area of the center shall also be protected. This includes locking manholes containing communications, electrical power, water, and natural gas facilities.

8.6 Server Room

Server Rooms, which may include Data Centers, Wire Closets or the Backroom, house critical information resources like servers, switches, routers, PBXs, wiring termination points, etc.

Note: The security requirements noted herein are designed to highlight important and relevant security aspects but should not be viewed as a comprehensive list on how to build a data center or server room, etc.

8.6.1 Physical Access

Entry to the Server Room and the following listed Server Room support facilities shall be restricted to personnel having a true business need for physical access.

1. Commercial power rooms
2. Emergency power rooms
3. Communications rooms
4. Cable vaults
5. Switch rooms
6. HVAC equipment rooms
7. Operations control rooms

NOTE: This paragraph applies to the Server Room, not necessarily the entire building which houses the Server Room.

All entrances and exits to the Server Room shall be controlled by a security system. Acceptable methods for controlling entry include guarded entrances, keyed physical access cards or keyed locks. The physical access controls shall be effective 24 hours a day, seven days a week.

Raised floors and suspended ceilings shall not allow physical access from outside the Server Room. Card readers and/or biometric devices should be used whenever possible to control access and record exit through all doors to the center.

8.6.2 Damage Control

The following controls shall be present in the Server Room:

1. Fire protection/detection systems, as required by code or internal NG9-1-1 Entity standards, shall be maintained and inspected at regular intervals. This includes, but is not limited to clean agent suppression systems, sprinkler systems, occupant hose systems, fire extinguishers and early warning fire detection systems.
2. If sprinkler systems are provided, fire retardant polyethylene sheeting shall be readily available for protecting media and equipment.
3. In other cases where water may be used for fire suppression or other water damage is possible, fire retardant polyethylene sheeting shall be readily available for protecting media and equipment.
4. Equipment cooling systems shall be installed and in good working order. Water sensing devices with alarms shall be positioned near valves of the cooling systems and other places where water is present.
5. Heating, ventilating and air conditioning (HVAC) systems shall be utilized to maintain the environmental conditions within the range required by the manufacturer of the systems equipment. There shall be dedicated HVAC system for the Server Room.
6. All critical information resources shall be on a UPS.
7. No food or drinks shall be allowed in any NG9-1-1 Entity Server Room.

8. No smoking is allowed in any NG9-1-1 Entity Server Room.
9. Storage of material under raised flooring is prohibited.
10. Storage of combustible material in the center is prohibited.
11. Furniture, storage cabinets, and carpeting shall be fire retardant.
12. Carpeting, if used, shall be anti-static carpeting.

8.7 Data Communications Networks

All data communications network elements shall be secured to the extent practical. Specific requirements must include, but are not limited to:

1. Hubs, routers, repeaters, bridges, firewalls, modems, ISDN bridges, network management consoles, patch panels, and other similar equipment shall be contained in locked rooms with appropriate physical access controls. If equipment is located in equipment rooms shared with non-NG9-1-1 Entity entities or in unsecured space, it shall be contained in locked cabinets.
2. Active network jacks and connections shall only be located in physically secured locations, i.e., NG9-1-1 Entity owned or leased space, in locked cabinets, or protected by locked physical barriers.
3. Unused network connections shall be removed or disabled in a timely manner.
4. Network media shall be selected and located so as to discourage wiretapping, electronic eavesdropping, or tampering, where feasible. This would include the use of fiber optic cable, coax, and/or enclosed conduit for cable runs.

9 Network and Remote Access Security Guidelines

This section addresses a number of security issues and risk mitigation strategies for networks in the NG9-1-1 Entity environment as well as connections allowing access into and out of those networks. These guidelines anticipate the very critical nature of the NG9-1-1 Entity mission and its importance to the general public for access to emergency services. The mission critical nature of the NG9-1-1 Entity is also discussed in the first section of this document.

9.1 Firewalls/Security Gateways

The NG9-1-1 Entity responsible for the network shall identify and classify network segments (e.g., call taker networks, CAD networks, etc) based on their business and technical functions so that the appropriate levels of protection can be configured for each segment. All boundaries or points in ingress and egress shall be clearly defined for every network. These may include external network connections, dual homed servers or other points of contact with other networks of different classification.

Firewall implementation guidelines shall include:

1. Firewalls shall be established at all boundary points to control traffic in and out of the network. All firewalls shall utilize a “fail all” final rule by default. Traffic shall be limited in both inbound and outbound directions by rules which specify source and destination addresses and destination ports. Stateful Packet Inspection firewalls shall be the minimum firewalls supported however, Application Layer Firewalls are strongly recommended. Simple “router” ACL rules are not sufficient as a “firewall.”

2. As part of the implementation of any firewall administration process, clear guidelines shall be established which indicate what services are permitted between endpoints. Since the base firewall policy is defined to be a “fail all” policy, no service shall be allowed without restriction on a perfunctory basis. (Note that a “deny all” policy, also known as a “white list” policy blocks all traffic by default.) However, access can be considered by the firewall administrator when presented with a business need request for the service. Such changes must be managed through a documented Change Control Process. The firewall administrator shall retain the right to escalate any such request via a documented escalation process if in disagreement with the request
3. Firewall rules generally consist of source and destination addresses and source and destination ports. In general, when an exception to a “deny all” rule policy is considered, these parameters shall be as tightly controlled as possible. At a minimum, restriction of source and destination IP addresses shall be specific to individual addresses. If more advanced technologies offer equivalent or better protection, they can be used. In some occasions, subnets or network ranges may be considered, but the security risks for every host or platform within the network range or subnet shall be evaluated.
4. The firewall administrator shall seek to minimize the number of ports exposed or permitted through the firewall.
5. All firewall administrators shall be highly qualified and experienced. Qualifications which shall be considered would include industry and/or vendor certifications with various firewall products. Additionally, the firewall administrator shall have an in-depth knowledge and/or experience in firewall support and management, various operating systems including application and operating system protocols (ports and sockets) and associated security implications. Other essential skills shall include networking, routing, LAN/WAN technologies and related security considerations.
6. Use of ports required by operating system or infrastructure functions and features across network boundaries shall be strictly controlled at the firewall. Examples include ports associated with NetBIOS, Directory Services, and file sharing.
7. All rules shall be reviewed periodically and at least once annually to verify continued need
8. Firewalls shall be assessed at a minimum of annually to address any service vulnerabilities which may have been identified since the previous inspection.
9. All firewalls shall log traffic on either a session (stateful) or packet basis. At a minimum, source and destination addresses and ports shall be captured along with relevant time stamps and action taken by firewall.
10. Whenever possible, log information shall be replicated off the firewall platform. Firewall logs shall be retained in accordance with applicable information retention guidelines.

11. Identification, authentication and access rights to log data shall be controlled as the log data may be required for evidentiary purposes and chain of custody shall be demonstrable.

9.2 Remote Access

Remote access is defined as a temporary connection from a user to an NG9-1-1 network from another location. Examples of remote access include, but are not limited to the following examples:

- Remote connection to the NG9-1-1 network for maintenance purposes
- Remote connection the NG9-1-1 network in order to use an application specifically designed for remote use (i.e. mobile call taking software)
- NG9-1-1 users remotely connecting into the NG9-1-1 network for management or administrative purposes.

No remote access shall be permitted to any NG9-1-1 network unless addressed by contract, employee policy or similar legal instrument which contains adequate security language as determined by a security professional.

9.2.1 Client Based VPN and Consolidated Modem Pool

All client based VPN and/or consolidated modem pools shall be operated by the NG9-1-1 security organization or personnel contracted for that purpose as they enable access from public networks such as the PSTN or Internet. Strict controls shall be maintained for VPN and/or consolidated modem infrastructures as they enable access to the NG9-1-1 Entity from public networks such as the Internet or public switched telephone network.

All client based VPNs shall utilize industry standard technologies which preserve data integrity and privacy while in flight. Examples of such technologies are IPSEC and SSL based VPN. Some tunneling protocols, while sound networking technologies, do not provide mathematical assurances of integrity and privacy, such as PPTP and L2TP.

All client VPN and centralized modem pool access shall utilize strong authentication which includes single use passwords.

All client VPN and centralized modem pool access shall be controlled by a firewall. Such firewall shall be able to utilize the user’s authenticated identity to impose access controls for that user and/or class of users (role based firewall policy).

All such access shall be logged. The log shall consist of authenticated identity, failed authentication attempts, time of attempted access, assigned IP addresses, time and date stamps, duration of access and internal locations accessed.

9.2.2 Directly Attached Modems

Use of modems which are directly attached to servers, routers, switches or other such equipment is strongly discouraged and generally prohibited by default in security best practice. However, certain conditions can be present which require their use. If needed, the usage shall be pre-approved, registered, documented and tracked in accordance with an exception process as documented in Section 12. Use of only "secured modems" shall be permitted. Uncontrolled use of modems can result in serious vulnerabilities and shall use risk mitigation measures.

When such modems are utilized through approved exception, they shall meet all criteria established for client based VPN or consolidated modem pools, including firewall access controls and single use passwords.

Directly attached modems shall use a third party authentication schema based on industry standards such as TACACS or RADIUS.

An accurate inventory of directly attached modems shall be maintained.

Other modem technologies which shall be considered include "dial/dial back", active only when primary access means is down or attached only to devices which have strong authentication mechanisms.

9.3 Extranet and External WAN Connectivity

External connectivity is often required to meet communication requirements for vendors and information sharing or other such purposes. Appropriate measures need to be taken to mitigate risks and exposures which may be introduced by such connectivity. Further, since these connections often leverage public transport media, information should be protected in flight, particularly if dedicated facilities are not utilized.

9.3.1 Private Lines and Dedicated Layer 2 Virtual Networks

Private facilities can be utilized and often provide a reasonable assurance of privacy such as point to point circuits (T1, fractional T1, DS-3, SONET rings, etc). Also lower layer partitions such as DLCI interconnection via Frame Relay and or VPNs via MPLS can provide reasonable assurances of privacy. Such communication facilities generally provide a high degree of reliability and use of multiple connections with different physical paths can provide even higher availability for critical communications. When possible the aforementioned network technologies should be considered in lieu of communication over public transport. Use of these network technologies does not necessarily preclude the need for end to end encryption. Organizations should evaluate the importance of the data traversing the network and determine if encryption is appropriate to meet the necessary privacy levels.

9.3.2 Private Communication over the Internet

Communication via the Internet has the potential to be intercepted and retained using trivial technologies such as network protocol analyzers and sniffers. As a result, the Internet does not offer any assurance of privacy. Unless measures are taken to protect the data in flight such as site to site or point to point VPN, any information transmitted via the Internet may be publicly or privately disclosed. Further, the identity of end points on the Internet cannot be determined with confidence.

However, these issues are well documented and a robust means exists to assure privacy of communication and the integrity of end points. Such solutions make use of tunneling protocols such as IPSEC and SSL. When communicating over public transport like the Internet communications shall be encrypted using IPSEC or SSL. When using such protocols, endpoint authentication shall be implemented using either certificates or similar credentials. Industry standard protocols shall be utilized and minimum key length shall be 128 bit.

9.3.3 External WAN Gateways

Since the external connection shall clearly be identified as an untrusted connection, a firewall shall be utilized to control the communication between the external endpoint or network and the internal NG9-1-1 environment. The firewall shall be implemented in a manner consistent with Section 9.1.

9.3.4 Demilitarized Zones (DMZs)

Certain applications (i.e. Web Servers, or email Bridgehead servers) may require access from external, public transport networks (i.e. Internet). These applications are commonly placed on special, external network segments commonly referred to as Demilitarized Zones (DMZs).

The DMZ provides intermediate environment for interaction with external domains without permitting access to internal domains or networks. This layering technique can improve the security posture of a system which requires an application to face the Internet without exposing the internal network.

When applications require access from external, public transport networks (i.e. Internet) they shall be placed on a DMZ, or shall be employ network based encryption and authentication mechanisms (i.e. VPN).

9.4 Intrusion Detection / Prevention

Use of network or host based intrusion detection or prevention technologies should be considered at network boundaries and/or on desired hosts. If used, they shall also be positioned on internal networks at strategic locations which may include high value networks such as those supporting call taking positions.

Intrusion detection/prevention signatures shall be routinely updated. Processes shall include well defined schedules for signature updates and shall include emergency update protocols for signatures required to detect high risk and day zero response events.

Intrusion Prevention technologies should be carefully deployed and implemented due to their automated response capability. False positive “hits” and related responses can result in interruption of legitimate traffic due to the automated responses. Careful design and configuration of intrusion prevention devices can help control these risks but not eliminate them.

It is recommended that Intrusion prevention technologies be implemented and managed by a security professional.

9.5 Layer 2 Security and Separation

Current network technologies permit different networks to share the same Layer 1 or physical facilities. Often these networks are called logical networks or multiple logical networks. This can include virtual router capability or VPN overlays over MPLS for virtual WANs or local LAN partitioning using VLAN or VRF technologies.

When such technologies are used, each VLAN, VRF or VPN shall be classified as required in Section 9.3. Once classified, these logical networks shall be treated as though they are different physical networks. All guidelines for use of firewalls, intrusion detection, remote access and all other relevant security principles shall be followed when designing interaction between virtual networks.

The equipment supporting virtual or logical networks can pose a unique risk. The routers and switches supporting these networks can be utilized as “islands” to hop between networks of different security classification. These risks can be managed using appropriate safeguards which may include the following:

1. All equipment supporting virtual or logical networks shall have a “management” tunnel for support and monitoring of the device.
2. Such equipment shall limit user group (write, read only, etc) access to particular virtual facilities whenever possible.
3. Commands (like telnet) which enable direct access between virtual facilities (sometimes known as “island hopping”) on the routers and switches shall be disabled or only allowed to be executed by the highest administrative privilege supported by the device. Such commands are typically vendor specific.
4. User access to devices supporting multiple virtual networks should utilize an industry standard authentication and access control protocol such as TACACS or RADIUS.
5. Layer 3 interactions between networks of differing security classifications shall only be done using a firewall or similar device

9.6 Network Redundancy and Diversity

9.6.1 Redundancy Considerations for On-Site/Local High Availability (HA)

Network redundancy is the duplication of equipment at a given site It can also include duplication of circuitry within a device such as control boards, power supplies, etc. Adequate redundancy can help avoid outages based on single hardware failure events. Typically protocols such as Virtual Routing Redundancy Protocol or Hot Standby Router Protocol are used to provide automated transfer of traffic between banks of equipment during failure events.

Traditional local HA in IP space can be handled by multiple elements:

1. Fast-action STP/RSTP/PVST+ re-converging redundant LAN switches or stacked LAN switches
2. Teamed NICs in servers and mission-critical desktop computers
3. If possible, redundant servers
4. HA firewalls
5. Redundant routers
6. Redundant WAN links
7. Out-of-band (OOB) communication links
8. Redundant premise wiring
9. Separate power feeds
10. Alternatives to commercial power.

Network redundancy can be difficult and expensive to design and implement, however, it is warranted when a very high degree of availability is required by the NG9-1-1 Entity. Network redundancy should be considered when implementing NG9-1-1 networks.

9.6.2 Diversity Considerations

Network diversity requires use of physically separate routing and cabling to provide further protection against outages triggered by a single event. Network diversity is more difficult and expensive to design and implement, however, it is warranted when a very high degree of availability is required by the NG9-1-1 Entity. The amount and nature of physical separation shall be clearly understood and defined for each location. Such separation may range from simple measures such as dual cable entrances on opposite sides of a given building to far more complex solutions such as different data centers in different cities. Routing protocols such as RIPv2, BGP and/or OSPF are used to perform automated transfer of traffic and/or service between physical locations.

Use of redundancy and/or diversity can have an effect on various types of security products. Most notably, traffic failover between different cities and different firewall sites can result in dropping sessions which are underway at the time of the failover. Applications shall be designed to elegantly recover such events and users advised as to proper “restart” procedures in case such a failover event was to materialize.

Network diversity should be considered when implementing NG9-1-1 networks.

10 Change Control and Documentation

Changes to the architecture, design or engineering of the NG9-1-1 networks shall include a formalized pre-cutover and post-cutover security review by the Local or Regional 911 security representative of NG9-1-1 Entity and any 3rd party vendors. A formal change control process shall be followed and appropriate documentation shall be produced and retained. If the change is complex, for example:

1. Connecting to a new untrusted/unknown network.
2. A new transport mechanism is used

3. A new authentication, authorization, accounting, or auditing framework is used
4. A new management ENTITY is used
5. A new IP allocation scheme is used
6. A new routing arrangement is used
7. A new security perimeter is redrawn

A team of Subject Matter Experts (SME) shall be assembled to review and approve the change.

11 Compliance Audits & Reviews

NG9-1-1 networks can be deployed in a number of different manners including; local, regional, national or even global. It is anticipated that initially local and regional NG9-1-1 networks will be deployed, and that the responsible agencies will develop appropriate policies (including security policies) for those systems. As national and/or global NG9-1-1 networks are deployed, it may become necessary to create organization(s) responsible for compliance auditing.

In the meantime, the agencies that deploy **NG9-1-1 networks** and develop security policies for them are required to conduct periodic audits or reviews to ensure that both the **NG9-1-1 networks** and the systems that are connecting to it comply with the security requirements listed in this NENA standard.

Audits can be conducted internally or externally. Internal audits are used to "self-check" an organization's compliance with security standards and/or policies. An external audit leverages a non-biased 3rd Party to independently perform the audit. Both methods are valid and useful.

- Internal Audits shall be conducted at a minimum of annually.
- External audits shall be conducted at a minimum of once every 3 years.
- Security audits shall utilize various methods to assess the security of networks and processes, applications, services and platforms including automated tools, checklists, documentation review, penetration testing and interviews.
- Findings resulting from such security assessments shall be subject to corrective actions. Such corrective actions shall be applied to the satisfaction of the organization managing the security assessments

NG9-1-1 Entities performing internal audits or “self-checks” may use external, 3rd party resources if necessary.

Findings resulting from such security assessments shall be subject to corrective actions. Such corrective actions shall be applied to the satisfaction of the organization managing the security assessments.

12 Exception Approval and Risk Acceptance Process

As the responsible agencies choose to adopt the security, requirements, and guidelines listed in this standard, there may be occasions when it is not possible to comply due to technical constraints, cost restrictions, or other reasons.

When such occasions arise, the resultant security risk shall be identified, documented and managed in accordance with the guidelines given below. **Be aware the non-compliance can put NG9-1-1 networks at risk. By signing an Exception Approval/Risk Acceptance Form, the NG9-1-1 Risk Acceptance Approver acknowledges that risk and that acceptance may absolve its service provider of any financial and liability responsibilities. Exception Approval / Risk Acceptance Forms should be included as a part of contracts or agreements if applicable.** It is highly recommended the NG9-1-1 Security Risk Manager and the Security Point of Contact get their legal and security organization involved when they have questions.

The exception approval and risk acceptance process shall consist of five phases:

1. **Risk justification**: Provides a business case for waiver or exception of the security requirement
2. **Risk identification**: Aims to thoroughly and unambiguously define the risk, the scope of what is at risk, and how the risk was identified.
3. **Risk assessment**: Uses three risk factors to assess: the potential severity of the risk, the impact of the risk, and the likelihood of the risk actually happening. These factors assist in deciding the mitigation of the risk, and in determining the frequency of review for the risk.
4. **Risk analysis**: Evaluates the feasibility and costs of different mitigation strategies relative to the potential cost impact.
5. **Risk acceptance and approval**: Only when risk cannot be totally removed or reduced to an acceptable level then it has to be accepted as is and get approval from NG9-1-1 Risk Acceptance Approver and include an Exception Approval/Risk Acceptance Form (EA/RAF).

All of the above shall be documented on the EA/RAF, including the names and contact information of the people who carried out the analysis.

12.1 Exception Approval and Risk Acceptance Process Scope

The exception approval and risk acceptance process shall be followed for *all risks* (e.g., security vulnerabilities cannot be fixed or security patch cannot be applied, cases of non-compliance with this Security Standard). .

The specific non-compliance or vulnerabilities documented in the EA/RAF shall be reviewed by NG9-1-1 Entity security organization and legal department. The actual form shall be maintained and tracked by the NG9-1-1 Entity Security Risk Manager, the Security Point of Contact (Security POC), and all involved parties.

Exceptions based on legal or regulatory requirements shall still be documented by EA/RAF form for tracking purposes.

12.2 Roles and Responsibilities in the Exception Approval and Risk Acceptance Process

The capture, assessment and management of a risk require the involvement of a number of individuals / teams who are required to fulfill certain roles. While others may be involved, there are three specific roles:

12.2.1 NG9-1-1 Security Risk Manager/Applicant

NG9-1-1 Entity shall assign a Security Risk Manager to manage security risk for NG9-1-1 network and who shall be responsible for completing the EA/RAF in a complete and accurate manner prior to submitting it to the appropriate Security Point of Contact / Team for review. The Security Risk Manager shall collaborate with other members of the pertinent security team in completing the form. The Security Risk Manager shall also obtain the approval signature from the NG9-1-1 Entity Risk Acceptance Approver.

The person filling the role of NG9-1-1 Entity Security Risk Manager/Applicant shall be an employee or an authorized agent acting on behalf of the NG9-1-1 Entity and may be determined in several ways. The Security Risk Manager may be, but not limited to, any one of the following:

1. The person identifying the need for execution of the exception approval and risk acceptance process with technical and business knowledge of the asset(s) at risk.
2. A system administrator, systems engineer, project manager or other key stakeholder with technical and business knowledge of the asset(s) at risk.

The NG9-1-1 Entity Security Risk Manager shall act as the point of contact for the organization owning the identified asset(s) at risk within the scope of the exception approval and risk acceptance process for the active duration of the EA/RAF. If the Security Risk Manager leaves the NG9-1-1 Entity or changes job responsibilities during the active duration of the EA/RAF, a new Security Risk Manager shall be identified to fill the role.

12.2.2 Security Point of Contact / Team

The Security Point of Contact / Team shall be responsible for reviewing the EA/RAF for completeness, accuracy and consistency given their experience and subject matter expertise. For high level risks, a team of Subject Matter Experts (SME) shall be assembled to review the EA/RAF and sign and document their concurrence position on EA/RAF prior to submission for NG9-1-1 Entity Risk Acceptance Approver's approval.

12.2.3 NG9-1-1 Risk Acceptance Approver

The senior manager (e.g., NG9-1-1 Entity Operation Manager or Director) within the NG9-1-1 Entity shall be responsible for signing to accept complete accountability for any identified risk. Responsibility for approvals shall not be delegated to subordinates or peers, and shall adhere to the management levels specified or higher. Generally, the appropriate senior manager for accepting the risk and approving the exception has financial and legal responsibilities for the services and operation of the specific NG9-1-1 Entity.

In cases where the assets at risk are not limited to a single device/application/network at one NG9-1-1 Entity location (e.g., it can potentially spread to associated NG9-1-1 Entity locations or other network domains), the EA/RAF reviewing Security POC / Security Teams may determine that the exception approval and risk acceptance shall be obtained from more than one senior managers. Assets that support multiple services may, as determined by the reviewing Security POC / Security Team, require concurrence from the Operations and Engineering senior management accountable for the availability and operability of the assets.

12.3 Process

Risks to NG9-1-1 are extremely important and they shall be acknowledged, assessed and managed according to their severity.

12.3.1 Process Flow

1. The NG9-1-1 Entity's Security Risk Manager identifies, justifies, assesses, and analyzes the risk. If the identification and/or analysis of the risk prove to be difficult, then a security team shall be contacted for assistance. The Security Risk Manager shall complete the EA/RAF, including Risk Justification, identifying the Security POC / Team, and NG9-1-1 Entity Risk Acceptance Approver.
2. The Security Point of Contact / Team shall assign the EA/RAF a globally unique tracking identifier / document number, review the form, determine or agree to who the NG9-1-1 Entity senior management approver is, discuss with Security Risk Manager until agreement reached or no more progress possible, involve a team of SMEs as necessary.
3. NG9-1-1 Entity Security Risk Manager signs EA/RAF.
4. The Security POC / Team documents concurrence position and signs the form
5. NG9-1-1 Entity Risk Acceptance Approver (senior manager) reviews the form, determines/documents strategy and reason, ensures risk mitigation is completed on the form, and accepts full responsibility and accountability by signing the EA/RAF.
6. The Security Risk Manager shall ensure the completed EA/RAF along with all necessary signatures/approvals, either physical or electronic, are filed with the reviewing Security POC / Team.
7. The Security Risk Manager, Security POC / Team, and Risk Acceptance Approver as well as other involved parties shall separately retain the form, either physical or electronic, for their records.

Risks being reviewed / renewed, i.e., not new, shall be thoroughly reviewed by the Security Risk Manager and reassessed by Security POC / Team prior to submitting to Risk Acceptance Approver/senior management to ensure that the information is current.

12.3.2 Tracking and Documentation

The required level of tracking/documentation is dependent on the time period in which the risk can be eliminated. See table below:

Risk Category / Severity	Time to Eliminate Risk	Risk Exists Less Than the Specified Timeframe and Minimum Required Level of Tracking	Risk Exists More Than the Specified Timeframe and Minimum Required Level of Tracking
Critical	Immediate action is required	Escalate until resolved	Escalate until resolved
High	30 days	Security POC / Team and all involved parties shall be kept informed of progress and Risk Acceptance Approver to be made aware by Security POC / Team	Full Documentation and Approval
Medium	60 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval
Low	90 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval

NOTE 1: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of an NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode.

NOTE 2: Once the risk category for a particular security risk is assessed, that risk level shall not be changed unless sufficient evidence is identified or there is justification for the change. All involved parties shall agree to the risk re-assessment before the start of the same exception approval and risk acceptance procedure. Risk category shall not be downgraded simply because it cannot be eliminated or reduced by the specified timeframe.

12.4 Review Period

All documented risks shall be periodically reassessed according to the associated risk category, and specified timeframes in the table below. If not then the EA/RAF expires leading to a state of non-compliance.

Risk Category	Review Period (months)
Critical	0
High	3
Medium	6
Low	12

Review period to be based upon the date associated with the first signature/approval of EA/RAF. Evidence of the approver's periodic reviews and continued approval and acceptance of risks shall be documented and submitted to the appropriate Security POC / Team then distributed to all involved parties. The EA/RAF shall be stored according to NG9-1-1 Entity and involved parties' record retention policy.

When a risk comes up for renewal, and a previously documented compliance action was not completed, the senior manager required for signature of the renewal shall be escalated to at least one level higher than before.

12.5 Change of Circumstance

Any change to the circumstances identified in the EA/RAF that will affect the associated risk, shall immediately be clearly documented in a revised EA/RAF, submitted to the appropriate Security POC / Team for review, and presented to the appropriate NG9-1-1 Entity Risk Acceptance Approver / senior manager for review and re-approval. Re-approval shall adhere to the same procedural formality as initial acceptance and approval.

12.6 Risk Identification

To ensure the capture of all relevant information in clear and meaningful terms, the identification of a risk can be divided in to a number of sub areas.

12.6.1 How was the Risk Identified?

There are various ways that network and computing security risks can be identified. For example:

1. A centralized Security Advisory authority (e.g., a NG9-1-1 Entity consortium staffed by their own security personnel or a service provided by a third party), report generated from local host IDS tool or local/remote vulnerability scan tool
2. Security compliance reviews, assessments, or audits: Security assessment of new or changed technology including product limitation, pre-production, post-production security review/assessment, security review program, new network connection/interface submissions, contract reviews, outsourced projects, ad hoc

discovery by the security organization, proposed new services, or non-standard customer requirement.

12.6.2 What is At Risk?

Some or all of the following will be required to fully describe the nature of what is at risk:

1. Service name(s), e.g., VoIP, MPLS/VPN, premise device management service, security management service, third party service
2. System process associated to the resources at risk, e.g., system change process, system patching process
3. Internal, commercial or outsourced service
4. Contract periods involved
5. Number of systems affected
6. Database system, middleware, application language, application name(s)
7. Number of users affected
8. Type of users affected, e.g., call taking position user, system administrator
9. Type of device, e.g., router, switch, workstation, server
10. Operating system(s), e.g., Windows 2000
11. Where are they physically located
12. What network(s) are they connected to, e.g., LAN, WAN

NOTE: It is important to consider not only what is placed at PRIMARY risk, that is the system(s), service(s), etc. directly at risk, but to also consider what if any system(s), service(s), etc. are at SECONDARY risk.

FOR EXAMPLE: When the risk under consideration relates to system(s) solely in support of a given NG9-1-1 Entity, e.g., a CPE firewall, it is essential that the risk analysis takes into account any risk to other NG9-1-1 Entity systems or services provided by others.

It needs to be clearly described exactly what is at risk, and the scope of assets at risk, e.g., class A versus class C IP address ranges, all systems on NG9-1-1 Entity's LAN versus just a single server in DMZ. In cases where the risk(s) are identified to span multiple assets, e.g., secondary systems, networks, multiple NG9-1-1 Entity's Risk Acceptance Approver / senior managers shall be required to approve the EA/RAF and accept accountability for the risk(s).

The version and section number(s) of non-compliance in the Security Guidelines document shall be fully defined in the EA/RAF. Along with details of the nature of the risk, the threat posed circumstances and the deviation from the Security Guidelines.

Attach all appropriate technical documentation, e.g., architectural diagrams or system descriptions, to support the risk identification and mitigation strategy.

12.6.3 Risk Assessment

In order to aid the consistent analysis of risk, and facilitate the comparison of the security risks a formal risk assessment model shall be used. This model derives a risk category from three (3) associated risk factors:

1. Vulnerability (in terms of both current and future contexts), i.e., what is the severity of the risk
2. Impact, i.e., what would it mean to NG9-1-1 Entity if the vulnerability were exploited, and
3. Threat, i.e., what is the likelihood of such an exploitation

NOTE: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of an NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode.

Also, during this time further risk assessment, analysis, and documentation may have to be delayed until the critical risk is resolved or mitigated.

Having assessed each of the three (3) risk factors in turn so as to assign them individual categories of: High, Medium or Low, they are then combined to obtain the overall risk assessment category:

1. High
2. Medium
3. Low

12.6.4 Vulnerability Assessment

Vulnerability assessment involves quantifying the severity of the risk being considered. Data to help in this assessment may come from using a security assessment tool (e.g., a vulnerability scanning tool, a local host IDS tool), having a security audit done by an authorized security company/organization, or security review by security SMEs.

In the event where more than one "What can be done" scenario exists, multiple vulnerability assessments (High, Medium, or Low) may be assigned. The highest rating takes priority.

Use the example table below to determine the vulnerability rating:

What can be done?	What type of User ID / access is required?	Vulnerability Assessment
Unauthorized access or improperly controlled	None	High

access through a filtering device.	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to an Administrative User ID.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to a Call Taking Position User ID.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to NG9-1-1 Sensitive (Restricted) or NG9-1-1 Sensitive (Most Sensitive Information) data.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to NG9-1-1 Sensitive (Internal Use Only) data.	None	Medium
	General	Low
	Administrative	-Not Applicable -
Denial of service attack affecting call taking position users or services those are not local to the device under attack.	None	High
	General	Medium
	Administrative	Low
Denial of service attack affecting only call taking position users or services that are local to the device under attack.	None	Medium
	General	Low
	Administrative	-Not Applicable -

In the example table above the following definitions are assumed:

1. Filtering device includes: Routers, firewalls, other network components and operating systems capable of restricting access through that device by means of filters, access control lists, etc. For example: Cisco router ACL, Checkpoint Firewall-1 rule set.
2. Administrative User ID: Any User ID having either system administrative, or security administrative authority. For example: UNIX root, Windows Administrator.
3. General User ID: Any User ID not falling into the "Administrative User ID" category.
4. NG9-1-1 Proprietary Data (Restricted or Most Sensitive Information)
5. NG9-1-1Proprietary Data (Internal User Only)

Where the above example table does not allow a reasonable assessment of the risk being considered, the NG9-1-1 Entity’s Security Risk Manager shall select a vulnerability assessment and document the justification for that selection.

NOTE: The above example table shall be used to assess what can be achieved rather than how it is achieved. So for example: If arbitrary code can be executed to gain UNIX root or Windows Administrator access, then it is the ability to gain root or administrator access that is important rather than that it was obtained by executing arbitrary code.

When documenting the reason for the vulnerability rating assigned include information about the purpose and capabilities of the assets, associated applications, current users and available access, trust relationships that could allow propagation, and any other information to provide full disclosure of the risk.

12.6.5 Impact Assessment

The impact assessment shall consider both direct and indirect impacts when determining the inventory of assets that could be affected. For example: A direct impact of a vulnerability when exploited may be unauthorized access to a given system and disclosure of information. However, an indirect impact may result if the unauthorized access can be used to gain further access to other systems in a networked environment.

When conducting an impact assessment, areas of impact should be analyzed using qualitative (e.g. loss of life, front page of the newspaper, etc) and quantitative means (e.g. financial loss, down time, etc).

12.6.6 Threat Assessment

Threat assessment involves quantifying the likelihood of the risk under consideration becoming a reality, that is, of it being exploited. Threat is actually a combination of two sub factors:

1. Capability, i.e., how able to carry out the attack are the attacker(s) likely to be. This will depend on the nature of risk and involves quantifying the sophistication and availability of hardware, software, skill, and knowledge necessary to exploit a given vulnerability. The threat assessment category shall also take into account any existing mitigation strategies in use that could lessen the threat, e.g., strong/one-time authentication, filters, etc.
2. Intent, i.e., how determined the attacker(s) are likely to be. This will depend upon the motivation of the attacker(s) and what benefits, e.g., financial, intellectual, revenge, that they think they will obtain.

NOTE: A state of full intent is always assumed, therefore, threat becomes capability.

The threat assessment of High, Medium or Low for a risk is determined as the most severe category for which any one criterion is satisfied. When documenting the reason for the threat rating assigned describe the sophistication and availability of hardware, software, skill, and knowledge necessary to exploit a given vulnerability. Identify all factors considered that could increase or decrease the ease of exploitation.

12.6.7 Determining the Risk Assessment Category

Risk Assessment involves the comparative assessment of available options. Documentation shall clearly articulate the possible corrective actions, their cost in time and resources to implement, their effectiveness for reducing or eliminating the risk, the residual risk that will remain, and the reduction in impact from exploitation that will result from each different option. Such that the

NG9-1-1 Risk Acceptance Approver / senior manager will be able to make a business decision based upon these facts.

The possible responses can be broadly grouped into four categories:

- Risk elimination
- Risk reduction
- Risk acceptance
- Risk transfer.

The information documented relating to each possible response shall be sufficient to ensure accurate costing, assessment and costing of residual risk, time to implement, possible constraints, and any other pertinent details. Regulatory requirements, technological issues, or performance implications may affect the decision to implement, or not implement, security measures. It is necessary to understand these constraints and document them in order to formulate and support the appropriate mitigation strategy.

12.6.7.1 Risk Elimination

From a purely security standpoint this is the preferred approach; however, even when this is supported by the business decision it shall be understood that it will take time to attain. The commitment for any expenditure or resource allocation that is necessary, and the planned date by which the risk will be eliminated shall be documented.

12.6.7.2 Risk Reduction / Mitigation

Risk reduction / mitigation can take various forms. Some of the options that shall be considered:

1. Contractual: For example, Non Disclosure Agreement (NDA), addition of stringent security requirements and audit rights
2. Physical: For example, enclosure of equipment within a locked cage, purchase additional hardware to separate computing environments
3. Logical: For example, add filters to restrict access (e.g., source IP address, protocol, application, SNMP MIB (Management Information Base) for Windows) implement or strengthen authentication (e.g., tokens, digital certificates), implement or strength authorization (e.g., read-only permissions, group restrictions)
4. Procedural: For example, call Network Operations Helpdesk before and after doing "X", add notification process when certain account access has been changed

As previously stated the implementation costs, timings and residual risks need to be considered for each option. Any mitigating controls that are in place shall be documented, along with the commitment for any expenditure or resource allocation that is necessary, and the planned date by which the risk will be reduced to the agreed upon level.

12.6.7.3 Risk Acceptance

The option of doing nothing to reduce the level of risk is not encouraged, but may in certain circumstances be appropriate owing to technical limitations, or prevailing business circumstances. **Any such acceptance of risk by NG9-1-1 customers shall be clearly documented in applicable contractual agreements.**

For the case where risk acceptance is used then residual risk rating will be as initially assessed and the potential impact cost should the risk occur would be as seen in the Section 12.6.5 Impact Assessment. Any mitigating controls that are in place shall be documented.

12.6.7.4 Risk Transfer

Risk transfer is generally covered under the state, local, or federal statue where applicable.

12.6.8 Fields on Exception Approval and Risk Acceptance Form

The following are the recommended sections and their associated fields to be included on the form.

1. Security Risk Manager – Detailed contact information
2. Risk Justification – a business case justifying the risk
3. Risk Identification – Description of risk (refer to Section 12.6 for detail) and date the risk was Identified
4. Risk Assessment – Rating (high, medium, low) for each assessment and the reason the particular rating is obtained
   a. Vulnerability
   b. Impact
   c. Threat
   d. Overall Risk Assessment rating (high, medium, low) is derived from the vulnerability, impact, and threat assessments.
5. Risk Analysis – Document the comparison between the cost of eliminating the risk with the cost of it becoming a reality (refer to Section 12.6 for detail)
6. Risk Mitigation – Document what strategy will be used, how, why, and when is it expected to last until. The exact approach (e.g., elimination, reduction, or acceptance) shall be clearly specified in this section.
7. Review Period – Based on the risk category (high, medium, low), re-review period of 3, 6, or 12 months will be assigned. Document the exact expiration date (from the date of the first signature on this form). **Make sure all parties involved are aware the re-approval shall adhere to the same procedural formality as initial exception approval and risk acceptance. Failure to review would lead to a state of non-compliance.**
8. Signatures – Sign to certify that this is an accurate assessment of the identified risk
   a. NG9-1-1 Security Risk Manager – Include name, NG9-1-1job title, organization, and date.
      a. Security Point of Contact (Security POC) / Team – Sign to certify concurrence that this is an accurate assessment of the identified risk only after the Security Risk Manager has signed. Include name, job title or organization name, date, conditional concurrence or non-concurrence, and any comments.

b. NG9-1-1Risk Acceptance Approver (or senior manager) – Sign to acknowledge approval of the identified risk only after the Security Risk Manager and Security POC/ Team have signed. By signing this form, this approver is **accepting complete accountability** for the identified risk and **commitment** to the plan as defined in the Risk Mitigation section. Include name, job title, and date.

See Appendix 4 for a sample risk acceptance and approval form.

NOTE: The Exception Approval and Risk Acceptance Form is an auditable record and copies must be retained by all signatories and affected parties for at least one year or longer according to regulatory requirements from closure of risk.

13 Incident Response &Planning

An Incident Response Plan shall be implemented. An Incident Response plan is defined as:

The formal, written plan detailing how an organization will respond to a computer security incident. Examples of security incidents include virus outbreaks, hacking attempts, critical service outages, denials of service, and more.

Responding to security incidents is an important part of an effective IT Security program. In order to rapidly detect incidents so as to minimize loss and destruction as well as restore service an incident response plan is necessary. Appendix 1 (Section 14.1) provides best practices and recommendations regarding the creation and execution of Incident Response Plans.

13.1 Appendix 1: Incident Response Planning

13.1.1 Incident Response & Planning

Responding to security incidents is an important part of an effective IT Security program. In order to rapidly detect incidents so as to minimize loss and destruction as well as restore service an incident response plan is necessary. An Incident Response plan is defined as:

The formal, written plan detailing how an organization will respond to a computer security incident.

Examples of security incidents include virus outbreaks, hacking attempts, critical service outages, denials of service, and more

This section is intended to provide personnel with the suggested procedures for identifying, reporting, and responding to computer and network security incidents.

This is applicable to:

- All personnel that perform functions or services that require securing information and computing assets.
- All devices and network services that are owned or managed by the service provider, vendor or NG9-1-1 Entity.

13.1.2 Background

Identification and reporting of computer and network security incidents shall be required to:

- Contain the incident and minimize the loss or compromise of information assets.
- Enable the initiation of the appropriate legal process.
- Correlate activity with other incidents to allow for coordinated action and to prevent duplicated efforts.
- Gather statistics for identifying trends and development of security measures to counteract vulnerabilities.
- Improve procedures and guidelines.
- Handle requests for security related information.

NOTE: All personnel shall notify the identified incident response service provider if any computer, computer system or network is compromised or if a breach of security is suspected or is in progress that involves internal network(s) and commercial network(s) owned and/or managed by service provider, vendor or NG9-1-1 Entity. It is important to note that regardless of the location where the suspected incident occurs or is observed, the identified incident response team shall first be notified. Security Point of Contact / Team will confirm the violation or make a record of it as appropriate and coordinate all further investigative and recovery efforts.

13.1.3 Roles and Responsibilities

A security agent shall be responsible for managing all investigative activities related to computer and network security incidents, and for managing the intrusion response effort. Investigative activities include, but are not limited to:

- Maintaining a list of SMEs, including name, department, contact information and areas of expertise.
- Contacting appropriate team members as needed in response to an intrusion.
- Coordinating intrusion response efforts,
- Interviewing witnesses,
- Reporting to management regarding an intrusion and response,
- Coordinating efforts with other organizations and other companies.
- Diagnose the event with the assistance of the local system administrator and determine the course of action to be taken.

13.1.3.1 Incident Reporting/Response Notification Contact Details

Any suspicious or unusual activity, which may indicate an attempt to breach the integrity of Public Safety's networks and systems, shall be reported immediately to an established Security Incident Response Team or equivalent. Any, and all, actual, attempted, and/or suspected misuse of Public Safety assets shall be reported immediately to the appropriate organizations.

All personnel shall be required to report all incidents to IR Service provider by one of the following methods:

- Hotline
- Website
- Email
- In Writing

All personnel shall use discretion when communicating suspicious activity, for example - do not send information about the attack via email if you suspect the computer or communication channel has been compromised. All personnel shall utilize the hotline to notify when online mechanisms are questionable, or the incident is of an urgent nature.

13.1.3.2 Intrusion Response Team

Responsibilities of the SME group assembled include, but are not limited to:

- Gathering and preserving evidence as it relates to intrusions,
- Providing evidence and evidence analysis to the security department, and
- Recommending changes to prevent and protect against future intrusions.

13.1.3.3 Asset Protection

Once the event is associated to a particular process, employee, contractor, vendor or other external ENTITY or individual, the group who is responsible for asset protection shall assume the responsibility for completing the investigation with the consultation and cooperation of the Security POC / Team. All members of the investigating team shall be expected to document their actions thoroughly, retain a copy of their notes for future reference, and submit a copy to the group who is responsible for asset protection to continue the investigation. The asset protection group shall retain all records, notes and reports in accordance with company retention guidelines. Evidence shall be protected, documented, and preserved once it is identified and seized. Any event being reported to law enforcement, or inquires from law enforcement, shall be coordinated by the asset protection group, excluding the normal subpoena submission process.

13.1.3.4 Managers

Management shall be aware and supportive of the additional responsibilities that their staff may have in association with the response effort.

13.1.3.5 Administrators

Administrators responsible for the day-to-day operations and/or security of information resources shall have the following responsibilities in connection with security intrusions:

- Confirming that an intrusion has occurred (or is occurring),
- Reporting the intrusion accordingly,
- Taking any immediate action as directed by Incident Response team,
- Keeping records of work efforts,
- Activating additional event logs,
- Where feasible, taking steps to prevent authorized entities from accessing the compromised system until evaluated.
- Cooperating in the investigation of the intrusion.

13.1.3.6 Detection and Response

If information resources are in danger of being irreparably harmed, the administrator shall take immediate action to protect these resources and implement the Business Continuity/Disaster Recovery (BC/DR) plan.

Examples of irreparable harm include, but are not limited to:

- An intruder has entered a system and is in the process of destroying or damaging data which cannot be recovered,
- An intruder is actively bringing systems down and impacting customer service, or
- An intruder is actively engaged in other behavior that will cause unrecoverable loss or damage to information resources.

Recommended actions include:

- Disabling all system accounts and/or changing all system passwords and /or disabling access permissions if allowed by the BC/DR plan,
- Correcting the vulnerability that allowed the intruder to gain access in the first place,
- Removing or shutting down the access method being used by the intruder,
- Bringing the system down or disconnecting it from the network, and
- Physically removing disk drives, tape files, or other system resources.

NOTE: If the NG9-1-1 Entity simply cannot shut the system down, then it shall go into a reduced production mode so the damage can be contained.

13.1.3.7 Information Disclosure

If a request for information is received, the appropriate security and legal organizations shall be contacted before responding. Personnel shall not disclose information about a security incident unless authorized by legal or Security Team.

Details relating to computer and network security incidents shall not be included in problem management records. Access to such details shall be controlled on a need to know basis.

NOTE: When proprietary information is inadvertently disclosed by Public Safety personnel, he/she shall immediately contact the Incident Response Team. The Incident Response Team shall contact Security Team if the information is security-related.

13.1.3.8 When to Contact the Incident Response/Reporting Team

The Incident Response/Reporting Team shall be contacted when:

- An active attack is detected.
- Activity which could be an attack is occurring.
- A suspected or actual security breach has occurred.

The following list of incidents is provided as examples only and is not considered comprehensive:

- Email related, such as: phishing, hoaxes, chain letters, hate mail, etc.
- Detection of Malicious code, such as: viruses, worms, Trojan horses, vulnerability exploits, etc.
- Web access related, such as: copyright violation, downloading prohibited files (music, video, etc.), etc.
- Intrusions – attempts (whether successful or failed) to gain unauthorized access to systems or data.
- Denial of service
- Inappropriate use of company equipment for processing or storage of data
- Compromise of system integrity or corruption of data – changes to system hardware, firmware or software without the owner’s knowledge, instruction or consent.

13.1.3.9 What Details to Report

Gather as much detail as possible to facilitate a timely and accurate assessment of the situation. Discussion of the situation shall be limited to those individuals with a direct need to know. The information outlined below is needed for incident response and investigation, it shall be provided if applicable:

NOTE: This is not an exhaustive list since each incident is unique.

- Point of contact for investigation.
- Originator of the incident, if this is not the same person as the contact person.
- Has this been reported before? Provide ticket number of previous reports or if reported to other organizations provide details.
- Is auditing turned on?
- If this involves customers provide details.
- Nature of the problem? Is the activity ongoing?
- Is there a backup of the affected system and is it available? (Not for use or disclosure outside NG9-1-1 Entity except under written agreement)
- What is the suspected business impact?
- What information has been exposed (Proprietary, etc.) and its classification if it is Proprietary in nature (This is important since suspected compromise of certain classifications of proprietary information could result in stringent individual notification processes involving privacy and legal involvement that would need to be initiated independent of this incident response process.)
- Identify the physical location of the assets involved.
- IP addresses and domain names of the machines involved (origination and destination).
- Network name to which the machine is connected.
- Date, time (including time zone), and duration of the activity.
- What is the suspected method of entry/origination?
- Operating system and patch level of systems involved.
- System clock time.
- System logs if available.

13.1.3.10 Next Steps

The Intrusion Response Team working with the appropriate Subject Matter Experts and representatives from other organizations shall perform the following steps:

- Discovery and report
- Incident confirmation
- Investigation and containment
- Recovery
- Post mortem and lessons learned

13.2 Appendix 2: Patching Best Results

The steps involved in applying security patches include:

1. Taking vulnerability advisories / security patch feed from various sources and/or (preferably) obtaining them from a consolidation service which performs vulnerability review and suggests priorities which can be a severity level and/or a target fixed duration, e.g., patch within 7 days
2. The devices' management authority receives notification of the patch or the vulnerability advisory and identifies the affected devices under his/her control.
3. Affected devices may be servers, desktops, Operating Systems, applications, middleware, network elements, and "black box" appliances which may have affected vulnerable components, e.g., application-specific call-processing equipment which uses Windows Operating System with .Net and SQL server.
4. A centralized security authority (which may be a NG9-1-1 Entity consortium owned security function or a service provided by a third party) assess the severity, risks involved, and production impact, then assigns the targeted fix duration
5. If a security vulnerability has a mitigation, please see #9 of the next section "General Patching Work Flow”.
6. If a security vulnerability cannot be fixed or a security patch cannot be applied (e.g., equipment vendor/integrator unwilling to address the security issues, patch breaks the application, patch is incompatible with the other device components, patch cannot address the issues, patch has not been made available, no support on end of life equipment, system owner refuse to upgrade for any reasons, etc.) within the specified "targeted fix period" while there is no mitigation existing, an exception form shall be filled with the risk-acceptance ENTITY clearly identified.
7. Theoretically, full-time completely isolated NG9-1-1 Entity environment (as a quarantined “clean room”) can be considered as a special case for exemption for few security deficiencies, such as not current in security patching practice. However, the defense of full time and completely isolated environment can hardly be maintained nor can be guaranteed, e.g., a service person brings in a laptop and connects to the supposing “isolated” local LAN or a person is plugging in a USB flash drive with unknown content into computer’s USB slot. Accepting the risks of using the “isolated air gap” as the mitigation has to be performed by the NG9-1-1 Entity owner as a business risk acceptance.

13.2.1 General Patching Work Flow

At this point, security patch is just a class of different patches. The following is a sample flow on a generic patch process. Note that a patch can be a regular feature enhancement upgrade, bug fixes patch (e.g., a service pack), or a security patch.

1. Devices' management entities related to the patch category (OS, application, middleware, etc.) have to test/verify the patch. Patch shall be obtained from its original source (usually from the software publisher itself.) If a device's patch

test/verification requires vendor/manufacturer assistance, proper procedure shall be used. Test/verification task shall not be performed in production environment and shall not affect the production activities.

2. Very often a patch may have a potentially broader impact than just limited to itself (e.g., an OS patch may break the application), all affected parties have to approve the patch or sent-back for corrective actions, e.g., fix the patch itself.
3. A "black box" appliance shall be patched and maintained by vendor responsible for such appliance. There is no special "exempt" status on such device.
4. Once a patch is approved, it is scheduled to be applied over one or more maintenance windows.
5. Patch shall be delivered to individual NG9-1-1 Entity using approved methods to ensure its integrity as well as to make sure the delivery channel/mechanism itself might not turn into a path of attack conduit or information leakage. Communication channel security is generally addressed within NG9-1-1 Entity networking architecture framework and the associated network security. The delivery mechanism may also include commercial couriers or hand-delivered. Content integrity can be assured by cryptographic checksum and digital signature.
6. Depending on the potential impact of the patch a full backup on the system may be needed.
7. Since NG9-1-1 Entity is a mission-critical environment, a rolling patching scheme or a phased patching scheme shall be pre-planned. It should be based on if the production tasks can be transitioned to or taken over by another device or function. If a single point of failure (SPOF) is identified, then alternative strategies as described in HA & BC/DR section shall be used.
8. As a common practice, any patch shall have a back-out/recovery procedure created, tested/verified, and fully documented. In the case of fault or instability caused by the patch, the back-out/recovery procedure shall be used to roll-back the environment to the state prior to patching activity.

NOTE 1: Certain production data/user data may be irreversible and cannot be recovered.
NOTE 2: due to vendor's own product design, certain patches are not reversible. In such case, full restoration can be considered.

9. If an issue (including security vulnerability) cannot be fixed for various reasons (e.g., patch breaks the application, patch is incompatible with the other device components, patch cannot address the issues, patch has not been made available, no support on end of life equipment, etc.) and an equivalent and equally effective mitigation method is available, it may be considered as the last-resort solution. Such mitigation shall be treated on a per-case basis. Mitigation shall be fully documented, tracked by document change-control process and time-bound such that when there is a fix, the proper way (i.e., patching) shall be used instead of taking the mitigation path.

13.2.2 Summary of Considerations

Important considerations include:

1. Controlling the pathway to get the patch into the environment
2. System impacts, e.g., will a reboot be required.
3. System outage, i.e., reroute the traffic for the duration of the update
4. Notification of all parties, e.g., vendor, NG9-1-1 Entity, Service Provider
5. Sequential patch implementation process.

13.3 Appendix 3: NG9-1-1 "Entity" Architecture, Design, Engineering Change Control and Documentation

13.3.1 NG9-1-1 1 "Entity" Architecture, Design, Engineering Change Control and Documentation

Within an NG9-1-1 "Entity", its internal network and associated security framework constitutes the core NG9-1-1 network architecture. Such intranet design may be further extended to other realms "NG9-1-1 network interconnection with other Network Domains diagram. NG9-1-1 "entities" may have multiple business relationships with other (mostly untrusted) Administrative Domain/Network Domains using IP wide-area network (WAN). The combined functions jointly performed by multiple domains form the architecture framework for E911 service.

13.3.1.1 Architecture Related to Inter-organizational Trust Relationship

Any trust, e.g., personnel, overall security posture, integrity of the networking, cannot be extended outside the local NG9-1-1 Entity organization or its "trust domain" without proper controls. Under careful review, there may be a subset of trust (e.g., allowing inter-NG9-1-1 Entity application-to-application data exchange after proper authentication, authorization, and accounting/auditing) can be established.

A classic case of extending the trust is the linking of Windows Networked Environment to another environment outside the local NG9-1-1 Entity.

Note that Windows Networking is a group of application-layer service based on ease-of-use and simplicity principle. A simple mouse "click" may have a potential extending the trust without this administrative user's full acknowledgement of the new risks just being committed. Thus by default such environment shall not be extended outside NG9-1-1 Entity boundary without addressing the security architecture and implementation sufficiently.

The standard security best practices are:

1. Use Application Firewall controlling Windows services riding on top of NetBIOS over TCP/IP (NBT)
2. Do not extend any Trust Relationship beyond local NG9-1-1 Entity's Windows Domain structure, i.e., broadening the security realm
3. Do not extend the Authentication, Authorization, and Accounting/Auditing (AAA) activity beyond the local NG9-1-1 Entity, nor shall accept others AAA result
4. Be careful on Active Directory structure and do restrict on information disclosure or unauthorized modification
5. Do not allow other Windows facilities (e.g., RRAS, Data Replication) outside the local NG9-1-1 Entity

13.3.1.2 Central-Server Based Communication

There are times certain communication methods will always go through servers hosted at Application Service Providers (ASPs) which serves as a switch board or relay host and information need to be passed through two end-points will go through the central server.

Some of the implementations are near real-time, while others are using a store-and-forward paradigm. In a mature service, such central servers perform tasks to ensure that service's production continuity, abuse avoidance, security enforcement, and cross-domain contamination suppression are all in place. One example is a sanctioned email service bureau, which will relay emails only after anti-spam filter, virus-scrubbing, and email content sanitization is applied.

For individual NG9-1-1 Entities, there may be resource constraints to deploy such a well-rounded central server to perform these complicated add-on functions. It certainly makes sense to use a sanctioned, security-approved service bureau as a service provider while individual NG9-1-1 Entities are simply subscribers of such service.

For new forms of communication, e.g., SMS, MMS messaging, pager, Blackberry, a gateway function shall be there to establish the linkage in between these messaging domains and the traditional IP-enabled service domain. Such gateway may be the most appropriate location to perform the necessary filtering and policy enforcement functions. The above example is used to illustrate how to include a new communication method into an acceptable NG9-1-1 Entity information feed.

As another example, Instant Messaging (IM) is a form of communication methods. Most of the IM services do go through a central server. A mature service provider does have some of the security enforcement features as described in secured email gateway above. Some of the service features (e.g., allowing transferring a file or installing a software) can be selectively turned-off. They are all driven by the central server configuration and policy applied. The common approach is to take the "Enterprise IM" solution where the policy is enforceable, the design is sanctioned, the user-community is controlled, and the peering user community (if it is allowed) is on the white-list.

13.3.1.3 Information Delivery Characteristics

One class of the communication methods is the store-and-forward delivery method[6] commonly known as "messaging". In this class, information (e.g., request for emergency assistance) may be relayed from one or more "relay hosts" with various delivery priorities before reaching the NG9-1-1 Entity domain. The end-to-end propagation delay may spread in between near-real-time to a lengthy (e.g., more than 12 hours) delay and there is no positive "Acknowledgment"

[6] Usually there is just one queue for processing/delivery. I.e., there is no priority treatment nor enforcement on prioritization

feedback[7] from the final intended recipient[8]. Actually, such message may even be scrubbed by a spam filter or anti-virus filter[9] anywhere en-route by a relay host. Bear in mind the end-user has to be trained to read[10] the message (e.g., email) within a short period acceptable by the E9-1-1 service.

Another communication method is near real-time, two-way interactive system. This can be a POTS call, VoIP call, online-chat (generic term: instant messaging), or TDD call[11]. The characteristic is there will always be a positive feedback by a 9-1-1 call-taker.

[7] Receiving an indication of "Message Sent" from an intermediate relay host does not mean the end point actually has received or the recipient seen the message

[8] Even if the final email server has received the message does not mean the actual person will (1) retrieve such message and (2) open-and-read such message

[9] A message might be deleted or placed in a quarantine folder, if it is been allegedly detected as carrying a virus.

[10] Message reader client software usually does not have an automatic priority screening function such that an emergency message embedded in the stream of messages can be moved ahead and read by the NG9-1-1 Entity call takers.

[11] This does not include call forwarded to an answering recorder system or an offline forwarder system, since these systems de-rate the response time equivalent to a store-and-forward system.

13.4 Appendix 4: Risk Acceptance & Approval Form

13.4.1.1.1.1.1 Request and Requestor Information			
Name			
Title			
Company			
Address			
Contact Number			
Email Address			
Date Requested			
Urgency	High	Medium	Low
Date Needed			
Duration of Risk	30 Days	60 Days	90 Days

Risk Justification:

Make a business case justifying the risk.

Risk Identification:

Description of the risk

Vulnerability Assessment:

Vulnerability	Type of Access (User ID) Required	Vulnerability Assessment
Unauthorized access or improperly	None	High
controlled access through a filtering	General	Medium
device.	Administrative	Low
Unauthorized access or improperly	None	High
controlled access to an	General	Medium
Administrative User ID.	Administrative	Low
Unauthorized access or improperly	None	High
controlled access to a	General	Medium
General User ID.	Administrative	Low
Unauthorized access or improperly	None	High
controlled access to	General	Medium
sensitive (Internal Use Only) Information	Administrative	Low
Unauthorized access or improperly	None	High
controlled access to	General	Medium
sensitive (Restricted) Information	Administrative	Low
Unauthorized access or improperly	None	High
controlled access to	General	Medium
sensitive (Most Sensitive Information)	Administrative	Low
Denial of service attack affecting systems,	None	High
users, or services that are not local	General	Medium
to the device under attack.	Administrative	Low

Denial of service attack affecting only systems,	None	High
users, or services that are local to	General	Medium
the device under attack.	Administrative	Low

Definitions for the above table:

- Filtering devices include: Routers, firewalls, other network components and operating systems capable of restricting access through that device by means of filters, access control lists, etc. For example: Cisco router ACL, Checkpoint Firewall-1 rule set.
- Administrative User ID: Any User ID having either system administrative, or security administrative authority. For example: UNIX root, Windows Administrator.
- General User ID: Any User ID not falling into the "Administrative User ID" category.

Impact Assessment:

Determine the inventory of assets that could be affected.

High Medium Low

Reasoning behind how the rating was obtained:

Threat Assessment:

Determine the likelihood of the vulnerability under consideration being exploited.

High Medium Low

Reasoning behind how the rating was obtained:

Overall Risk Assessment:

Determine the overall level of risk based on the combined ratings of Vulnerability, Impact, and Threat Assessments.

High Medium Low

Risk Analysis:

Document the comparison between the costs of eliminating the risk with the potential losses posed by the threats.

Risk Mitigation:

Document what strategy will be used, how, why, and when is it expected to last until. The exact approach (e.g., elimination, reduction, transference, or acceptance) shall be clearly specified in this section.

Review Period:

Based on the Overall Risk Assessment (High, Medium, Low), a re-review period of 3, 6, or 12 months will be assigned. Document the exact expiration date (from the date of the first signature on this form). **Make sure all parties involved are aware the re-approval period. All parties shall adhere to the same procedural formality as initial exception approval and risk acceptance. Failure to review leads to a state of non-compliance.**

Signatures:

Sign to certify that this is an accurate assessment of the identified risk

13.4.1.1.1.1.2 *NG9-1-1 Security Risk Manager*	
Name	
Title	
Organization	
Date	
Signature	

Sign to certify concurrence that this is believed to be an accurate assessment of the identified risk only after the Security Risk Manager has signed.

13.4.1.1.1.1.3 *Subject Matter Expert*	
Name	
Title	
Organization	
Date	
Signature	

Sign to acknowledge approval of the identified risk only after the Security Risk Manager and the Subject Matter Expert have signed. By signing this form, this approver is accepting complete accountability for the identified risk and commitment to the plan as defined in the Risk Mitigation section.

13.4.1.1.1.1.4 *NG9-1-1 Risk Acceptance Approver (Executive or Senior Manager)*	
Name	
Title	
Organization	
Date	
Signature	

14 Previous Acknowledgments

NA, this is Version 1.