Policy #: 911-013
Previous Policy #: ETS 12-001
Effective Date: April 12, 2012
Revised: May 14, 2019, March 12, 2025

Information Technology and Network Security Policy

TABLE OF CONTENTS

1. INTRODUCTION:

In order to provide a secure 9-1-1 information and network system to the public safety agencies of the DuPage Emergency Telephone System Board [DuPage ETSB], the DuPage ETSB 9-1-1 System is committed to providing a secure yet open network that protects the integrity and confidentiality of information while maintaining its accessibility.

2. POLICY:

Each member of the DuPage ETSB is responsible for the security and protection of electronic information resources over which the agency has control. Resources to be protected include networks, computer/workstations, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-site entities must comply with the same security requirements as in-house activities and receive prior approval from the DuPage ETSB.

3. ROLES AND RESPONSIBILITIES:

Responsibilities range in scope from security controls administration for a large system to the protection of a user's own access password. A particular user often has more than one role.

3.1 Agency Administrative Officials (individuals with administrative responsibility for public safety agencies must:

- Identify the electronic information resources within areas under their control;
- Define the purpose and function of the resource;
- Establish acceptable levels of security risk for resources by assessing factors such as:
    - How sensitive the data is, such as arrest data or information protected by law or policy,
    - The level of criticality or overall importance to the continuing operation of the system as a whole, individual departments, units or other essential activities ,
    - How negatively the operations of one or more units would be affected by the unavailability or reduced availability of resources,
    - How likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
    - Limits of available technology, programmatic needs, costs, and staff support,
- Ensure that requisite security measures are implemented for the resource.

3.2 Providers [individuals who design, manage and operate the agency's electronic information resources, e.g. project managers, system designers, application programmers, or system administrators) must:

- Be knowledgeable regarding relevant security requirements and guidelines;
- Analyze potential threats and the feasibility of various security measures in order to provide recommendations to the 9-1-1 System Coordinator and the ETS Board members;
- Implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative policy;
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements.

3.3 Users (individuals who access and use DuPage ETSB 9-1-1 System resources) must:

- Be knowledgeable regarding relevant security requirements and guidelines;
- Protect the resources under their control, such as access passwords, computer/workstations, and data they download.

Insufficient security measures at any level may cause resources to be damaged, stolen, or become a liability to the system. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, computer/ workstations(s) posing a threat will be blocked from network access. (Section 10: Guidelines and Procedures for Blocking Network Access specify how the decision to block is made and the procedures involved.)

4. KEY SECURITY ELEMENTS

4.1 Logical Security: Computer/ workstations must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks.

Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk. Attention must be given not only to large systems but also to computer/workstation(s) which, if compromised, could constitute a threat to the agency's or 9-1-1 resources, including computer/workstation(s) maintained for a small group or for an individual's own use.

4.2 Physical Security: Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a User's display screen.

5. PRIVACY AND CONFIDENTIALITY

Applications must be designed and computer/ workstation(s) must be used so as to protect the privacy and confidentiality of the various types of electronic data they process, in accordance with applicable laws and policies. Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured network system to a User's location, adequate security measures must be in place at the destination computer/workstation to protect this "downstream data". Technical staff assigned to

ensure the proper functioning and security of 9-1-1 resources and services are not permitted to search the contents of electronic communications or related transactional information not owned or managed by the DuPage ETSB 9-1-1 System. For example, any scanning of network traffic to detect intrusive activities must be used in a way to protect any personal information that may be captured during the scanning for possible intrusive activities and must be in compliance with laws and policies protecting the privacy of the information.

6. COMPLIANCE WITH LAW AND POLICY:

Departments, units, or groups should establish security guidelines, standards, or procedures that refine the provisions of this Policy for specific activities under their purview, in conformance with this Policy and other applicable policies and laws. The following activities are specifically prohibited under this Policy:

- Interfering with, tampering with and/or disrupting resources;
- Intentionally transmitting any computer/workstation viruses, worms, or other malicious software;
- Attempting to access, accessing, or exploiting resources the user is not authorized to access;
- Knowingly enabling inappropriate levels of access or exploitation of resources by others;
- Downloading sensitive or confidential electronic data/information to computer/workstation(s) that are not adequately configured to protect the system from unauthorized access;
- Disclosing any data/information that the user is not authorized to be disclosed.

7. DEPARTMENT SECURITY CONTACT POLICY

7.1 Purpose The purpose of this policy is to ensure that DuPage ETSB public safety agencies can be contacted in the event of a computer/ workstation or network security incident. The ability to quickly contact responsible departmental personnel and have them take appropriate action can mitigate the negative effects of an incident both locally in the department and more globally throughout the DuPage ETSB 9-1-1 System.

7.2 Background Risks to the DuPage ETSB 9-1-1 System are very serious. The loss or corruption of information or access to information on workstations and servers could greatly hinder public safety work. The DuPage ETSB 9-1-1 System has a responsibility to secure its computer/ workstation(s) and networks and to respond quickly to threats to the integrity of systems and data. A compromised computer/workstation in one department can easily be used as a springboard to launch attacks on computer/workstation(s) in other departments. Because of these risks, DuPage ETSB 9-1-1 System personnel must take action when they become aware of a security incident specifically involving a DuPage ETSB 9-1-1 System computer/workstation. In cases where the incident poses a potentially serious threat to 911 information system resources, the computer/workstation will be immediately blocked from network access.

When a problem computer/workstation is identified, whether or not it is blocked from network access, DuPage ETSB 9-1-1 System personnel must be able to quickly contact someone in the appropriate public safety agency who can take action and/or pass the information on to the appropriate departmental support personnel. Quickly reaching a departmental contact is also important so that any affected user(s) may be informed of the situation. In addition, DuPage ETSB 9-1-1 System personnel will inform this contact person of possible irregularities such as computer/workstation(s)

with configuration problems that could negatively impact the network or that appear to be infected with a virus.

7.3 Requirements To implement this procedure, each agency needs to appoint a contact and one or more backup contacts. All contacts for a given agency should be reachable through a single phone number. Contacts must respond to incident reports from DuPage ETSB 9-1-1 System staff and pass them on to responsible departmental or third party support personnel as appropriate. Contacts need to have some familiarity with the computer/workstation(s) in their department and be able to determine who a responsible technical person is; it is not necessary for the contact to have extensive security expertise. Security contacts are responsible for ensuring that appropriate personnel take action in response to each security incident (including escalating the incident to an appropriate departmental authority if action is not taken) and that resolution of each incident is reported to the DuPage ETSB 9-1-1 System Administrator.

8. MINIMUM SECURITY STANDARDS FOR NETWORK DEVICES

8.1 Summary

Access to and use of the DuPage ETSB 9-1-1 System network services are privileges accorded at the discretion of the DuPage 9-1-1 Emergency Telephone System Board. Devices connected to the DuPage ETSB 9-1-1 System network must comply with the minimum standards for security set by the DuPage ETSB 9-1-1 System Coordinator. Devices that host restricted data are required to conform to more rigorous security standards. Agencies may develop stricter standards for themselves. Devices that do not meet minimum standards for networked host security configurations may be disconnected.

8.2 Who Should Read this Policy

- Chiefs and Department Heads;
- System Administrators;
- Users: Individuals working with networks, computer/workstations, workstations, software and data.

The Chief and/or Department Head shall be responsible to execute the User Form [Appendix D] which serves as acknowledgement and responsibility for the users of their agency. The Chief and/or Department Head shall submit the User Form to the DuPage ETSB 9-1-1 System Manager within 60 days of receipt of this policy. Executing this document for the agency ensures that the Department Head, System Administrators and Users have read this policy. Failure to submit the User Form can result in the DuPage ETSB 9-1-1 System Manager blocking access to the Network system until compliance is met. [Section 10] This form will be updated annually. However, changes in the contact information should be submitted immediately to the DuPage ETSB 9-1-1 System Manager on a new form.

8.3 Why We Have a Minimum security Standard for Network Devices

The DuPage ETSB 9-1-1 System encourages the use of its network in support of Public safety. However, this resource is limited and vulnerable to attack. The DuPage ETSB, therefore; reserves the right to deny access to its network by devices that do not meet its standards for security. This policy requires compliance with minimum security standards to help protect not only the individual device, but other devices connected to the DuPage ETSB 9-1-1 System network. The policy is also intended to prevent exploitation of DuPage ETSB 9-1-1 System resources by unauthorized individuals.

The policy applies to all devices connected to the 911 network or using a DuPage ETSB 9-1-1 System Internet Protocol (IP) address to originate communications. Devices include computer/workstations, printers, or other network appliances, as well as hardware connected to the 9-1-1 network from behind firewalls or Network Address Translation (NAT) systems.

8.4 Responsibilities

8.4.A DuPage ETSB 9-1-1 System Manager:

- Pursuant to County Ordinance 20-40 Internal Operations (a)(3) may create a Tech Focus Group and designate an ETSB staff member to lead this focus group;
- Provides direction, planning and guidance about information security;
- Develops and reviews DuPage ETSB System information security policy and procedures;
- Oversees the creation of the minimum security standards for network devices with technical staff;
- Approves exceptions to minimum security standards;
- Works with the users in the public safety community to protect computer/workstation(s), devices, and the 9-1-1 network infrastructure from electronic attack;
- When necessary, blocks access to the 9-1-1 network in accordance with *Guidelines and Procedures for Blocking Network Access.*

8.4.B Agency Administrative Officials:

- Shall ensure that devices connected to the 9-1-1 network from their department are supported by an administrator or user with the ability to maintain minimum security standards.

8.4.C System Administrators:

- Are the designated person(s) within an agency with the ability to maintain minimum security standards;
- Shall ensure compliance with the minimum security standards set forth in the *Procedures* section of this policy;
- Such assigned person(s) for the agency will provide contact information to the DuPage ETSB. If an agency does not provide contact information, the designee will be the department head.

8.4.D Departments, Users and Individuals:

- Shall ensure that they use devices that comply with the minimum standards set forth in this policy;
- Function as the system administrator in the absence of an assigned system administrator;

9. PROCEDURES

9.1 Minimum Standards

Minimum security standards for devices attached to the DuPage ETSB 9-1-1 System network are attached in this document as Appendix A: Minimum Standards for Security of DuPage ETSB 9-1-1 System Networked Devices. These standards change periodically. Network device users should consult the DuPage ETSB 9-1-1 System Office to make sure they have the latest security standards before upgrading or changing their equipment. Implementing guidelines that provide more information about complying with minimum security standards are attached to this document as Appendix B page 17: (Implementing Guidelines for the Minimum Standards for Security of DuPage ETSB 9-1-1 System Networked Devices).

9.2 Exceptions
Departments, units, or individuals unable to comply with the minimum security standards for the DuPage ETSB 9-1-1 System networked devices but wishing to connect to the network must identify resources that will assist them (on an ongoing basis) in becoming compliant. Devices that do not comply with the minimum standards are subject to exclusion from the 9-1-1 network. Departments, units, or users who believe their devices require configurations that do not comply with the minimum security standards for 9-1-1 networked devices may request connection to the 9-1-1 network on an exceptional basis. Requests for such exceptions should be directed to the System Administrator, which will process the request for final approval by the 9-1-1 System Coordinator.

9.3 Revising Minimum Standards
Changes to the minimum security standards for networked devices will be approved by the 9-1-1 System Coordinator of the DuPage ETSB 9-1-1 System.

10. GUIDELINES AND PROCEDURES FOR BLOCKING NETWORK ACCESS

10.1 Purpose
DuPage ETSB 9-1-1 System administrators must take immediate action to mitigate any threats that have the potential to pose a serious risk to DuPage ETSB 9-1-1 information system, resources or public safety databases. If the threat is deemed serious enough, the computer/workstation(s) posing the threat will be blocked from network access. These guidelines specify how the decision to block is made and the procedures involved.

10.2 Guidelines
DuPage ETSB 9-1-1 System personnel have the authority to evaluate the seriousness and immediacy of any threat to DuPage ETSB 9-1-1 System information, system resources or public safety databases and to take action to mitigate the threat. Action that is taken will be responsible and prudent based on the risk associated with that threat and the potential negative impact to the DuPage ETSB 9-1-1 System caused by making the offending computer/workstation(s) inaccessible. Examples of threats that are serious enough to invoke these procedures are:

- The level of network activity is sufficiently large as to cause serious degradation in the performance of the network;
- System administrative privilege has been acquired by someone who is not supposed to have it;
- An attack on another computer/workstation or network has been launched;
- Confidential, private or proprietary electronic information or communications are being collected;
- Continued complaints have been received regarding inappropriate activity and no response has been received from the departmental contact regarding the incident.

10.3 Procedures
Users can be blocked from the network system:

1. If they fail to complete the User Form [Appendix D].
2. If the threat is immediate, the offending computer/workstation(s) will be blocked immediately and notification will be sent to the department Chief Administrator immediately that the block has occurred.

3. If the threat is not immediate, notification of the threat will be sent to the department Chief Administrator via email. If a response is not received within 4 hours indicating that the department is taking action to mitigate the threat, the offending computer/workstation(s) will then be blocked.

In instance 1, execution of the User Form is required. In instance 2 or 3, the DuPage ETSB 9-1-1 System personnel will work with the department Chief administrator and/or the system administrator(s) to ensure that the computer/workstation(s) are properly re-secured. If a block has been put in place it will be removed when both the department and DuPage ETSB 9-1-1 System personnel agree that the problem causing the incident has been sufficiently addressed.

10.4 Recourse
If a department feels that a computer/workstation has been inappropriately blocked it may request a review of the decision by the 9-1-1 System Coordinator. If, after the review, there is still a disagreement with the decision, it may be further reviewed by the DuPage Emergency Telephone System Board.

11. UTILIZATION OF DUPAGE ETSB 9-1-1 PUBLIC SAFETY APPLICATIONS AND NETWORK EQUIPMENT

11.1 DuPage ETSB 9-1-1 Public Safety Applications
The DuPage ETSB provides and manages several public safety application systems for use with Emergency 9-1-1 dispatch services.

The use of these systems is restricted to authorized personnel. The use of these systems by unauthorized personnel may result in the blocking of specific computer/workstation(s) and/or the disabling of user accounts. Additional information regarding the proper use of DuPage ETSB 9-1-1 public safety applications can be found in Appendix D.

11.2 DuPage ETSB 9-1-1 Network Equipment
The DuPage ETSB provides and manages equipment for use with Emergency 9-1-1 dispatch services. The equipment includes but is not limited to;

- Computer Aided Dispatch (CAD) and CAD workstations;
- Mobile for Public Safety (MPS)
- UPS battery backup systems;
- Network routers and switches;
- Telephone voice loggers;
- Customer Premise Equipment (CPE)
- DuPage Emergency Dispatch Interoperable Radio System (DEDIR System) Consoles
- Fire Station Alerting (FSA)
- LiveMum

11.2.2 DuPage ETSB 9-1-1 Network Equipment - Interfaces
- Interfaces and interface management

This section addresses interface connections to the 9-1-1 system. This section outlines the system requirements for the interface connections. The Tech Focus Group has recommended that there

should not be any direct connections to the production CAD system. Each interface request will be reviewed by the Tech Focus Group both before and after implementation to ensure the security and reliability of the submission.

Real Time Interfaces
The current CAD system utilizes *Edge Frontier (Xalt Interface),* which is designed to handle these types of interfaces. *Edge Frontier (Xalt Interface)* allows the applications to receive information without impacting the security and performance of the 9-1-1 System. An *Edge Frontier (Xalt Interface)* interface would be developed and maintained by Hexagon for all non-9-1-1 interfaces at the cost of the requesting agency.

Asynchronous Interfaces
For this type of interface, a secondary archive server will be utilized to provide the data requested. This data provided is not real time.

The use of this equipment for any purpose other than that intended by the DuPage ETSB is prohibited and may result in computer/workstations(s) being blocked from the DuPage ETSB 9-1-1 Network system..

11.3 DuPage ETSB 9-1-1 Network Communications Systems
The DuPage ETSB 9-1-1 communications networks were implemented to provide Emergency 9-1-1 dispatch services through public safety applications. To provide a secure and accessible communications network the DuPage ETSB shall restrict network connectivity and only permit access to approved systems. These restrictions shall be implemented through the use of network firewalls and access control lists. All DuPage ETSB 9-1-1 public safety applications listed in section 11.1 and Appendix D are considered approved.

Any system not owned or managed by the DuPage ETSB shall be considered unapproved and will be blocked from the DuPage ETSB 9-1-1 network communication systems without specific approval by the DuPage ETSB. To obtain approval for network access by a system not owned or managed by the DuPage ETSB agencies will be required to complete the DuPage ETSB 9-1-1 Network Systems Access Request Form which can be found in Appendix G. Additionally, agencies will be required to submit a Memorandum Of Understanding – Information Technology and Network Security Access, authorized and executed by their appropriate corporate authorities or a department head that has the designated the authority to approve it. The Memorandum Of Understanding – Information Technology and Network Security Access can be found in Appendix H.

Revision approved: _____
Greg Schwarze, Chair

Revision adopted on: _____

APPENDIX A: Software Patch Updates

DuPage ETSB 9-1-1 System networked devices must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed. Exceptions may be made for patches that compromise the usability of critical applications.

What are "security patches" and why do I need to keep my software up-to-date?
Security patches are updates to software that eliminate vulnerabilities that, when exploited, will compromise the security of the device. These updates are required for operating systems, application software, firmware, or any other software operating on the device. The majority of devices that are compromised are done so through the exploitation of security vulnerability that could have been eliminated with an already-released security patch. Almost every major worm or virus outbreak could have been prevented had users applied current security patches.

What does "software for which security patches are made available in a timely fashion" mean?
If security vulnerability is found for a piece of software, a software update that eliminates that vulnerability must be made available in a timely fashion. If an update is not made or will not be made within a reasonable amount of time, that software cann**ot** run on the networked device. The DuPage ETSB 9-1-1 System Administrator is responsible for determining whether or not a security patch is being "made available in a timely fashion".

What if my critical software cannot be patched, will I be blocked from the network?
An agency or device may be blocked from accessing the network unless the agency system administrator requests an exception from the DuPage ETSB 9-1-1 System Administrator and your request is granted. If the application is determined to be critical but contains a security vulnerability that warrants a network block, an exception will most likely require the mitigation of the vulnerability through other means.

How do I ensure that my software has all currently available security patches installed?
It is very important to keep yourself apprised of security updates to all of the software on your machine. The easiest way to do this is to check the ETSB Extranet site on a regular basis.. Information about how to join this list, if it exists for the application, will almost always be available on the vendor or developer's site. The following types of software are *most* likely to contain security vulnerability and should therefore be *more* frequently checked for patch currency (i.e. weekly):

- Operating Systems
- Server Software - Web servers, Mail servers, FTP servers, Database servers, etc.
- Web Browsers - Internet Explorer, Netscape, Safari, Mozilla, etc.
- Email Clients - Outlook, Outlook Express, Eudora, Netscape, Mozilla, etc.
- Peer-to-Peer File Sharing software - Kazaa, Gnutella, eDonkey, etc.

APPENDIX B: Minimum Standards for Security of DuPage ETSB 9-1-1 System Networked Devices

The following minimum standards are required for devices connected to the DuPage ETSB 9-1-1 System network.

Software patch updates
DuPage ETSB 9-1-1 networked devices must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed. Exceptions may be made for patches that compromise the usability of critical applications.

Anti-virus software
Anti-virus software must be running and up-to-date on every level of device, including clients, file servers, mail servers, and other types of DuPage ETSB 9-1-1 networked devices.

Host-based firewall software
Host-based firewall software must be running and configured according to the "Implementing Guidelines for the Minimum Standards for Security of DuPage ETSB 9-1-1 System Networked Devices", on every level of device, including clients, file servers, mail servers, and other types of DuPage ETSB 9-1-1 networked devices. While the use of departmental firewalls is encouraged, they do not necessarily obviate the need for host-based firewalls.

Passwords
DuPage ETSB 9-1-1 System must identify users and authorize access by means of passwords. When passwords are used, they must meet the Minimum Password Complexity Standards. In addition, shared-access systems must enforce these standards whenever possible and appropriate. All default passwords for access to network-accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

No unencrypted authentication
Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the 911 network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all 911 devices must use only encrypted authentication mechanisms unless otherwise authorized by the DuPage ETSB 9-1-1 System Administrator. (See "Requests for Exception" in the DuPage ETSB 9-1-1 System Policy on Minimum Standards for Networked Device Security Configurations.) In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

No unauthenticated email relays
DuPage ETSB 9-1-1 System devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Authenticating the machine (e.g. IP address/domain name) rather than the sender is not sufficient to meet this standard. Unless an unauthenticated relay service has been reviewed by DuPage ETSB 9-1-1 System Administrator and approved as to configuration and appropriate use, it may not operate on the 911 network.

No unauthenticated proxy services
Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration. Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by the DuPage ETSB 9-1-1 System Administrator and approved as to configuration and appropriate use, it is not allowed on the 911 network.

Physical security
Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 30 minutes.

APPENDIX C: Implementing Requirements for the Minimum Standards for Security of DuPage ETSB 9-1-1 System Network Devices

I. **Procedure for Participating Agencies for Mobile Computers.**

a. As a condition of access and use of the network, DuPage ETSB will provide access to and require agencies to download the Network optimization software and register their mobile computers in order to have access to the 9-1-1 System network.

- Agencies must have unrestricted wireless cards connecting to the network.
- ETSB will block internet access while connected into the system ("restrict" the card), if the agency requests it.
- The Absolute Secure (fka: NetMotion) software provides access to the following systems that support or receive information from the 9-1-1 system only:
  - CAD system and interfaces 9-1-1 services
  - State systems that support 9-1-1 services
  - County applications supporting 911 services
  - Approved Agency systems that support 9-1-1 services
  - Approved PSAP systems that support 9-1-1 services
- ETSB will review any additional software systems.

b. DuPage ETSB acknowledges that certain member agencies already have network optimization systems in place. Agencies with existing network optimization systems will be allowed to continue use of their systems as long as they meet all the requirements in this policy and the security policy.

II. Procedures for connecting to the network inside stations.
As a condition of access and use of the network, computers must comply with all system requirements. Requirements will vary depending on individual components in 9-1-1 system.

- To ensure network security, Agencies shall submit compliance documentation for the above requirements to DuPage ETSB via an email to the ETSB ticketing system..
- The Technical Team will review the documentation and; if needed, may schedule a meeting with the requesting agency to review their request. The Technical Team will then make a recommendation to the DuPage ETSB Executive Director on the security and reliability of the submission for connection to the 9-1-1 network.
- The ETS Board authorizes the 9-1-1 System Manager to approve compliant applications pursuant to this policy. Disputed applications that cannot be mitigated, shall be brought to the ETS Board.

III. **Quality Assurance Process**
When approved, DuPage ETSB will require on demand, read-only access to the agency systems connecting to ETSB resources. DuPage ETSB staff will conduct random compliance checks and document compliance.

DuPage ETSB reserves the right to deny agencies the ability to connect to the ETSB network if at any time DuPage ETSB determines the reliability and stability of the network is jeopardized.

Agencies should immediately advise DuPage ETSB of any changes to, maintenance to or failures of their security and systems which could impact the stability and security of the 9-1-1 network. Notification can be made to the on-call ETSB technician.

Passwords
DuPage ETSB 9-1-1 System must identify users and authorize access by means of passwords. When passwords are used, they must meet the Minimum Password Complexity Standards. In addition, shared-access systems must enforce these standards whenever possible and appropriate. All default passwords for access to network-accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

Minimum Password Complexity Standards:
All passwords employed to authorize access to 911 systems or services must meet the following standards: The password MUST:

- Contain eight characters or more;
- Contain characters from at least two of the following three character classes:
  - Alphabetic (e.g.: a-z, A-Z)
  - Numeric (i.e. 0-9)
  - Punctuation and other characters (e.g.: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

The password MUST NOT be:
- A derivative of the username.
- A word found in a dictionary (English or foreign).
- Names of family, pets, friends, or co-workers.
- Computer/workstation terms and names, commands, sites, companies, hardware, or software.
- Birthdays or other personal information such as addresses or phone numbers.
- A set of characters in alphabetic or numeric order (e.g. abcdef), in a row on a keyboard (e.g. qwerty), or in a simple pattern (e.g. 123123).
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., qwerty1, 1qwerty).

Why do I need a strong password?
Passwords are used for various purposes. Some of the more common uses include: local accounts, web accounts, and email accounts. A weak (or absent) password is one of the most common ways for an attacker to compromise your account; therefore, you should be aware of how to select strong passwords.

The standard requires that devices must be configured to enforce the minimum password complexity requirements "whenever possible and appropriate". What type of situations might be exceptions?

It may be inappropriate in situations where the device is single-user (home machines or laptops). While you MUST use a password that meets the complexity requirements, it is not necessary to configure the device to enforce the requirements on these single-user devices.

What are some other password guidelines?

- Passwords should never be written down or stored on-line.
- In general, a password should be as long as possible while still being easy-to-remember. One way to do this is create a password based on an easy-to-remember phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!
- You should change your passwords on a regular basis, at least every six months.

No Unencrypted Authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the 911 network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all 911 devices must use only encrypted authentication mechanisms unless otherwise authorized by the DuPage ETSB 9-1-1 System Administrator.

What is encrypted authentication and why should I use it?

Many Internet services such as email, calendaring, and file sharing require some kind of authentication before you can use the service. That is some way for you to prove that you are who you say you are. That's typically done with a simple user ID and password. There are, unfortunately, several pitfalls in implementing this over a network. One of the biggest problems is that the Internet is designed in such a way that makes it fairly easy for a hacker to "listen in" on other peoples' communications. So, for example, every time you (or your email client) authenticate to an email server your user name and password is sent over the network to the server. That means that anyone listening in would see your user name and password. They would then have full access to your email account and could abuse it in a myriad of ways including sending out spam, viruses, or worse in your name.

To avoid this, you need to make sure that your user name and password are always encrypted before being sent over the network to the server. How you do this depends on the type of service you're using and generally requires the provider of that service to configure the server in such a way that it can accept encrypted connections.

No Unauthenticated email relays

In addition to causing problematic bandwidth usage and inappropriate email appearing to come other unauthorized activities, in a manner similar to "virus" attacks.

No Unauthenticated proxy services

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration. Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by the DuPage ETSB 9-1-1 System Administrator and approved as to configuration and appropriate use, it is not allowed on the 911 network.

Physical Security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 30 minutes.

What is physical security with respect to networked devices, and why is it important?
Physical security prevents attackers from accessing a device physically rather than through the network. It is even more important than network security, but is often overlooked by users and administrators. Regardless of the level of protection that a device has from network-borne attacks, physical access to the device by a knowledgeable attacker will almost always result in a complete compromise.

What do the Minimum Standards require?
The Minimum Standards for Security of DuPage ETSB 9-1-1 System Networked Devices require that, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 30 minutes.

What does "where possible and appropriate" mean? Only some devices are capable of "locking" after a set amount of time and requiring a user to re-authenticate. On devices where it is possible, it is sometimes inappropriate or unnecessary. For example:

- CAD terminals
- If the activation of the "locking" mechanism interferes with essential software in a way for which it was not designed (e.g. a password-protected screen saver that crashes critical lab equipment monitoring software and disrupts research)

Note: "where possible and appropriate" does not mean "where you feel like it", and annoyance at having to type a password more frequently does not constitute a valid reason to deem it inappropriate to do so.

Why 30 minutes?
It's long enough to prevent users from having to type their password in so often that it becomes a major annoyance or that passers-by are given too many opportunities to see the user typing it in. On the other hand, it's short enough to give attackers a reasonably small window under which they could access and compromise the device. There may be situations under which a shorter time-frame may be appropriate.

APPENDIX D: Utilization of Public Safety Applications on the DuPage ETSB 9-1-1 System Network

What public safety applications does the ETSB provide and manage on the DuPage ETSB 9-1-1 System Network?
The DuPage ETSB provides and manages several public safety applications for use with E9-1-1 dispatch services. These applications are listed below.

- Closed Public Safety Network
- Computer Aided Dispatch (CAD)
  - CAD is used by E9-1-1 dispatchers to record E9-1-1 incidents and dispatch public safety resources.
- Mobile for Public Safety (MPS)
  - Mobile for Public Safety is used by public safety resources to communicate remote from the field.
- Audio Logger
  - Recording of telephone and radio transmissions
- Customer Premise Equipment (CPE)
  - E9-1-1 ANII/ALI equipment or NG911 software and hardware used to receive, process and dispatch 9-1-1 calls. "ANI/ALI" stands for "Automatic Number Identification" and "Automatic Location Identification," which are technologies used in 911 systems to automatically display a caller's phone number (ANI) and their corresponding address (ALI) when they make a call, allowing emergency dispatchers to quickly locate the caller's location without needing to ask for it manually; essentially, it's a system that identifies both who is calling and where they are calling from.
- Fire Station Alerting Equipment (FSA)
  - A fire station alerting system is a communication and dispatch tool by integrating with audio and digital signals in real time.
- DuPage Emergency Dispatch Interoperable Radio System including portable and mobile radios and radio consoles in dispatch
- Fire Recommendation Software
  - Recommends optimal unit relocations or “move-ups” that reflect the standardized coverage policies of the system users

What can I use these applications for?
The DuPage ETSB 9-1-1 public safety applications may only be used for public safety purposes. Accessing any DuPage ETSB 9-1-1 public safety application for personal use is strictly prohibited.

Who can use the DuPage ETSB 9-1-1 Public Safety Applications?
Authorized users will be granted user accounts by the DuPage ETSB Systems Administrator. Each user account may only be used by the user it was created for. Sharing user accounts or accessing a DuPage ETSB 9-1-1 public safety application with another individuals user account is strictly prohibited.

What data can I access within a DuPage ETSB 9-1-1 Public Safety Application?
Users are restricted to data granted by their user account. Accessing or attempting to access data outside of the configured security privileges or data owned by a different DuPage ETSB agency is strictly prohibited.

APPENDIX E: Utilization of DuPage ETSB 9-1-1 Network Equipment
What equipment does the DuPage ETSB provide for use with the DuPage ETSB 9-1-1 Network Systems?

The DuPage ETSB provides equipment to facilitate the use of the DuPage ETSB 9-1-1 public safety applications and connectivity to the DuPage ETSB 9-1-1 communications networks.

The DuPage ETSB provides CAD workstations to PSAP locations for use with the CAD and MPS system. Policies for the proper use of these workstations can be found in the CAD Workstation Acceptable Use Policy.

The DuPage ETSB provides network routers and switches to connect PSAPS to the DuPage ETSB 9-1-1 communications networks. These network devices are owned and managed by the DuPage ETSB and any modifications or unauthorized connections are strictly prohibited.

Information Technology and Network Security Policy
Policy No: 911-013 – APPENDIX F

User Form

Agency:	
Address:	
Chief/Department Head:	
Telephone:	
Email address:	
System Administrator:	
Telephone:	
Celllular Phone:	
Email address:	

With the submission of this form, I confirm that the users of the above listed agency have reviewed and understand the DuPage ETSB Information Technology and Network Security Policy, Policy No: 911-013, [the "Policy"]. The users of the agency further understand that, for security purposes, under the guidelines of this policy that an agency computer/workstation may be blocked from the DuPage ETSB 9-1-1 System Network if a violation of the policy is initiated. This form further certifies that the computer/workstations connection to the DuPage ETSB 9-1-1 System are in compliance and/or that this agencies is working with DuPage ETSB technical staff to gain compliance.

_____
Date:

_____
Authority:

_____
Chief/ Department Head

This agency is also a PSAP: [ ] yes [ ] no

APPENDIX G

TO: Emergency Telephone System Board 9-1-1 System Manager
FROM:
SUBJECT: Interface Request Form

Type of Interface (select one)

	Real Time Interface
The current CAD system utilizes *Edge Frontier (Xalt Interface),* which is designed to handle these types of interfaces. *Edge Frontier (Xalt Interface)* allows the applications to receive information without impacting the security and performance of the 9-1-1 System. An *Edge Frontier (Xalt Interface)* interface would be developed and maintained by Hexagon for all non-9-1-1 interfaces at the cost of the requesting agency.	
	Asynchronous Interface
For this type of interface, a secondary archive server will be utilized to provide the data requested. This data provided is not real time.	

With the submission of this form, I confirm that I reviewed and understand the DuPage ETSB Information Technology and Network Security Policy, Policy No: 911-013, [the "Policy"]. I understand that an MOU will be required and there may be fees and costs involved for any interface that is not 9-1-1 related.

_____ _____
Signature Date:

_____
Print Name of Agency Head

Please include a short description or attach a copy to this request for the following:

- **Technical Requirements:** (will also be reviewed by Tech Focus Group)
- **Desired Project Implementation Schedule:** (include/attach a go-live goal or schedule)
- **Vendor Service Level Agreement (SLA)** (It is important that ETSB know the hours of work)

Agency:	
Agency Contact:	
Email:	
Cellphone:	
IT Administrator:	
Cellphone:	
Email:	
Vendor Name:	
Contact:	
Cellphone:	
Email:	
Interface:	

Internal Review

Recommendation:
Yes = Support of Request
No = Oppose Supporting the Request. (a No Recommendation will provide a brief summary of the opposition to the ETS Board submitted via the 9-1-1 System Coordinator)

Yes No

[ ] [ ] **Tech Focus Group Recommendation**
- [ ] Technical Requirements received
- [ ] Project Improject Implementation Schedule received
- [ ] Vendor SLA received

[ ] [ ] **9-1-1 System Manager**
- [ ] MOU executed

[ ] [ ] **ETS Board Approved**: _____ Chair's Initials:_____
Date

APPENDIX H

Memorandum of Understanding
Information Technology and Network Security Access
By and Between
The Emergency Telephone System Board of DuPage County ("DuPage ETSB")
And
_____ ("Agency")

This is an agreement between the DuPage ETSB, an Emergency Telephone System Board created pursuant to 50 ILCS 750/ *et. seq.* and the Agency governing the use of the DuPage ETSB network.

I. Purpose and Scope

The purpose of this agreement between the parties is to formalize a usage agreement for access to the DuPage Emergency Telephone System (ETS) network in accordance with DuPage ETSB policy 911-013 ("Policy"), attached and incorporated as Attachment A, and made a part of this Agreement as if fully set forth herein.

II. Background

The DuPage ETSB 9-1-1 communications networks were implemented to provide Emergency 9-1-1 dispatch services through public safety applications. To provide a secure and accessible communications network the DuPage ETSB shall restrict network connectivity and only permit access to approved systems. These restrictions shall be implemented through the use of network firewalls and access control lists. All DuPage ETSB 9-1-1 dispatch-related public safety applications listed in section 11.1 and Appendix D of DuPage ETSB policy ETS-12-001 are considered approved.

III. Responsibilities of the Agency

The Agency wishes to have access and to connect to the DuPage ETSB network for an application that is not listed in DuPage ETSB policy ETS-911-013.

Through the execution of this document, the Agency attests and affirms that:

1. They are or will be compliance with DuPage ETSB policy 911-013;
2. They have completed and submitted the appropriate request documents contained in 911-013 and are attached hereto as part of this Memorandum of Understanding;
3. They agree to abide by the conditions set forth in DuPage policy 911-013. To the extent that the Agency's current technology does not meet the policy requirements, the Agency agrees to meet the requirements upon replacement of equipment and/or within twelve (12) months of the execution of this agreement. The Agency understands that failure to comply will result in termination of the interface/connection to the DuPage ETSB network.
4. They will notify DuPage ETSB in writing within 30 days of their intent to termination this Memorandum of Understanding.

5. The Agency agrees that it will not allow access to the DuPage ETSB network to any other party through the Agency connection.

IV. Responsibilities of DuPage ETSB

DuPage ETSB agrees to support, maintain and make available access to the DuPage ETSB network to the Agency until or unless by mutual agreement of the Agency and DuPage ETSB the Agency opts to discontinue its connection.

DuPage ETSB will provide the Agency access to the DuPage ETSB network. Access shall be provided at no cost to its members whose surcharge is remitted and retained by DuPage ETSB. Costs to members who surcharge is remitted to another entity or non-members shall be determined through negotiation and separate contractual agreement.

All costs associated with the connection/interface to the DuPage ETSB network is the sole responsibility of the Agency.

With respect to Section III, Item 3, the DuPage ETSB agrees to provide the Agency with 30 days written notice. prior to the ETSB's termination of an interface/connection, Notwithstanding the forgoing, the DuPage ETSB may terminate the Agency's software application if the ETSB determines that such application poses an immediate threat to the security of the DuPage ETSB network. The DuPage ETSB shall provide notice to the Agency's submitted single point of contact as previously communicated to the ETSB if any such termination takes place.

V. Further Agreements of the Parties

DuPage ETSB agrees to provide reasonable notice to the Agency of any changes or upgrades to the network or a system application which may interrupt access. Any costs related to a change or upgrade for an interface or Agency application is the sole responsibility of the Agency. DuPage ETSB will not delay a system change or upgrade for its users of public safety 9-1-1 systems.

VI. Term, Termination, and Modification of Agreement

This Memorandum shall become effective upon its execution by both parties remain in effect until terminated as provided herein. The Agency may terminate its participation in the agreement within thirty (30) days of its execution.

Emergency Telephone System Board of
DuPage County

By_____
Chair

Date:_____

_____
The Agency

By_____
Authorized Agent

Date:_____