Eversource Energy Emergency Response Program
PLAN

Eversource Cyber Security Plan

EP-ALL-PLN-1100

Revision 10

Approved Process Owner:

Signature: 

Name: Christopher Leigh

Date: August 15, 2025

Title: Vice President & Chief Information Security Officer

Effective Date: August 15, 2025

Applicability: Eversource

EVERSOURCE

Ensure you are using the current revision by verifying it against the controlled electronic copy located in the Emergency Response Program Documentation Lotus Notes Database.

Intentionally Blank

Table of Contents

1. CONCEPT OF OPERATIONS 5
1.1 Purpose 5
1.2 Overview and Cyber Security Approach 5
2. Risk Management 6
2.1 Overall Enterprise Risk Management Program 6
3. Asset, Change, and Configuration Management 9
3.1 Critical Asset Identification 9
4. Identity and Access Management 10
4.1 Establish and Maintain Cyber Access 10
4.2 Physical Access Controls for Employees and Vendors 11
5. Threat and Vulnerability Management 12
5.1 Existing Systems 12
5.2 New Systems 13
5.3 Outside Services 13
5.4 Security Patch Assessment 13
5.5 Security Patch Management 13
5.6 Vulnerability Assessment Process 13
6. Situational Awareness 15
6.1 Logging 15
6.2 Monitoring Electronic Access 15
7. Information Sharing and Communications 16
7.1 Cybersecurity Threat Information Sharing 16
7.2 Information Protection Policy 16
7.3 Data Protection 16
8. Event and Incident Response, Continuity of Operations 18
8.1 Data Breach Program 18
8.2 Business Continuity Plans 18
8.3 Disaster Recovery Plans 18
8.4 All Hazards Plan 18
8.5 Eversource All Hazards Emergency Response Plan 19
9. Supply Chain and External Dependencies Management 20
9.1 Procurement Security Controls 20
9.2 Compatibility with Existing Equipment within the Enterprise 20
9.3 Adherence to Architecture Standards 20
9.4 Adherence to Standard Procurement Processes 20
9.5 Network Security Perimeter and Access Control 20
9.6 Vendor Security Program Evaluation 21
10. Workforce Management 23
10.1 IT Security Organization 23
10.2 Personnel Risk Assessment 23
10.3 Awareness Program and Training 23

11. Cybersecurity Program Management 25
11.1 Standards Based Security Program 25
11.2 Cyber Security Risks and Mitigation 25
11.3 CIS Governance 25
11.4 IT Security Organization 26
11.5 Architecture to Protect Critical Systems: Defense in Depth 26
11.6 Architecture to Protect Critical Systems: Boundary Defense/Electronic Security Perimeter 26
11.7 Architecture to Protect Critical Systems: Malicious Software Prevention 26
11.8 Account Management 26
11.9 Cyber Vulnerability Assessment 27
11.10 Disposal or Redeployment 27
11.11 Cybersecurity Plan Updates 27
12. RECORD OF CHANGES 27

Attachments

Attachment 1 Acronyms and Abbreviations 28
Attachment 2 Reference Documents 30

1. CONCEPT OF OPERATIONS

1.1 Purpose

The Eversource Cybersecurity Plan is a high-level overview of Eversource's Cybersecurity Program. The program is structured using the ES-C2M2 model and covers all systems and assets at the Enterprise Level. The detail and rigor of cybersecurity controls get stronger based on the criticality of the system that Eversource is protecting. The specific details of the security program are confidential and can only be shared with third parties when appropriate controls are in place (for example, at an Eversource location with legal contracts in place).

1.2 Overview and Cyber Security Approach

Eversource Energy's overall approach to cybersecurity follows the National Institute of Standards and Technology (NIST) framework. Use of the NIST framework ensures that security measures and risk management efforts align appropriately with the priority of business processes for which Eversource is responsible. The framework also provides a common means of organizing Eversource's diverse array of cybersecurity activities to prevent gaps in coverage. It also enables a rigorous and integrated process for managing a necessarily complex Information Technology (IT) environment and melding it with business needs, risk management processes, and all of the various resources that are applied to effective cybersecurity. The Corporate Information Security (CIS) services, policies, and standards apply to all business units and operating entities. Each operating entity also has specific security requirements in place to address specialized technology used within each service territory (such as different software and hardware used in control systems in the field). Eversource applies leading security principles and practices to protect the infrastructure and computer networks from cyber-attacks. This includes a *defense-in-depth* strategy where *best of breed* specialized security technology is used, such as host- and network-based firewalls, intrusion detection/prevention systems, virus and anti-malware protection, file encryption, content filters, network segmentation, and vulnerability scanners to further reduce risk of compromise. The Eversource control centers architecture is consistent with the recommendations from the Department of Homeland Security's (DHS) *Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies* (October 2009). In addition, Eversource includes the key recommendations to the enterprise network where appropriate.

Various aspects of this cyber security program are periodically assessed using internal and external expertise to ensure effective operation. CIS enforces this security architecture with strict policies and procedures. Corporate policies regarding definition and use of sensitive information include:

- Internal Controls and the Safeguard of Company Assets Policy
- Code of Business Conduct
- Critical Infrastructure Protection Policy
- IT Vulnerability Management Policy
- IT Access Administration Policy
- Corporate Information Security Procedure
- Eversource Privacy Policy

Critical Infrastructure Protection (CIP) asset information is defined by the North American Electric Reliability Corporation (NERC) standards. CIP version 5 has been implemented effective July 1, 2016. CIP-003-CIP Cyber Security Policy-POL-01 sets forth requirements for the Eversource CIP program. Approximately 60 underlying procedures exist for the CIP program.

2. Risk Management

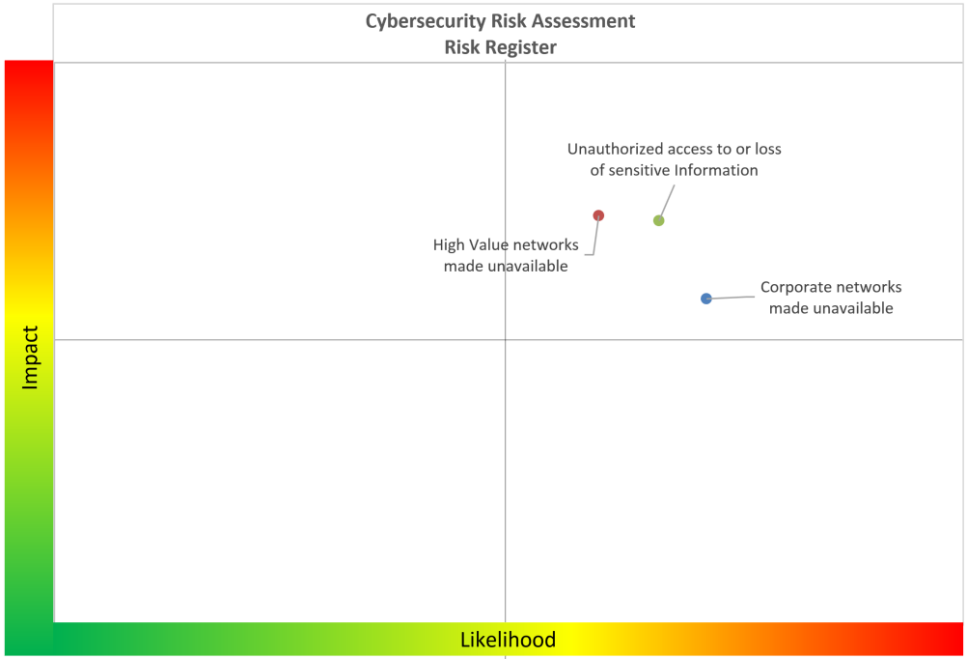
The objectives of the risk management processes are to establish, operate, and maintain an enterprise risk management program to identify, analyze, and mitigate risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

2.1 Overall Enterprise Risk Management Program

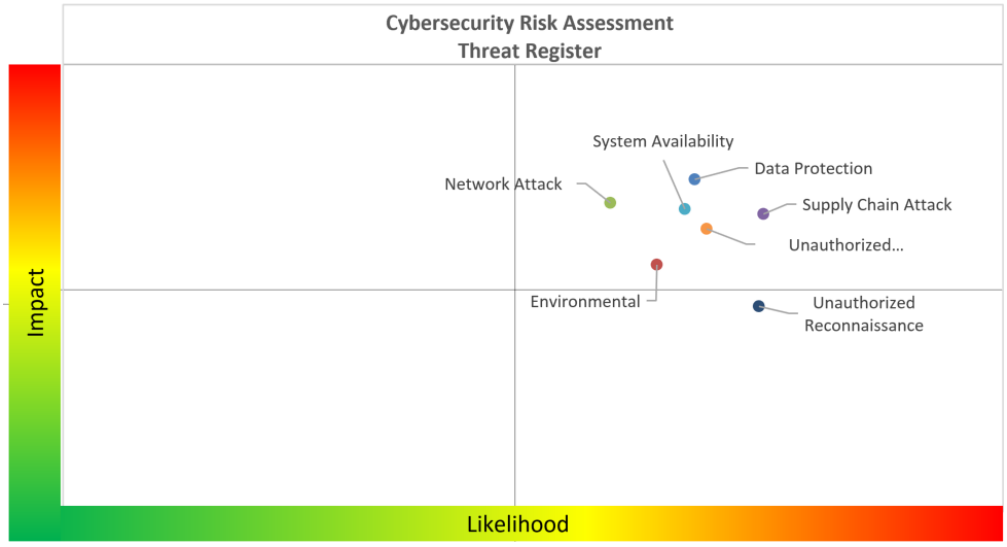
Within the overall risk management program, cybersecurity risk is considered as an enterprise corporate risk through the risk assessment process conducted by the Enterprise Risk Management Department (ERM). The ERM program involves the application of a well-defined, enterprise-wide methodology designed to allow the Risk Committee, comprised of the senior officers and directors, to oversee the identification, prioritization, mitigation, and reporting of principal business risks such as cybersecurity. The ERM program is integrated with other assurance functions throughout Eversource, including Compliance, Auditing, and Insurance to ensure appropriate coverage of risks that could impact the company. To support the ERM process, the Information Security team performs annually, a detailed Cybersecurity Risk Assessment based on the NIST 800-30. This assessment includes reviewing known threats and the Eversource Cybersecurity Risk register to assess areas requiring additional mitigation plans. The Information Security organization also identifies emerging risks to the company, through participation in industry groups, discussions with management and in consultation with outside advisers. Eversource management analyzes the risks to determine materiality and other attributes such as likelihood, impact, and mitigation strategies. Management broadly considers the Eversource business model, the utility industry, the global economy, and the current environment to identify risks. The findings of this process are periodically discussed with the Finance Committee of the Board of Trustees as well as with other Board Committees or the full Board of Trustees, as appropriate including reporting on how these issues are being measured and managed.

2.2 Cyber Security Risk Management Program

As a subset of the ERM program, an Annual Risk Assessment has been developed based on the NIST 800-30 standard. This process evaluates threat actors and the likelihood that an attack will occur. In addition, an assessment of the impact is done. The various threat scenarios roll up into the Risk Register which summarizes the top company cyber risks and top threats. The model is updated for new threat scenarios and if necessary, the Risk Register. An example of the summary results follows:



Example Only



Example Only

The results and new risks are discussed with Executive management based on the criticality of the event. Communications may be immediate email/phone calls through formal presentations to executive management, including the Board of Trustees

For all new technologies, the procurement process includes an assessment process for vendors. This process begins with a questionnaire completed by vendors relating to their security policies, personnel security, environmental security, network management, end-point security, access control, compliance, business continuity and disaster recovery planning, and application security (External Vendor Due Diligence Questionnaire). Vendors are provided access to an IT Security Requirements portal to assist them in understanding what is required of them.

All new initiatives for technology are evaluated based on the content of a formal questionnaire referred to as the Corporate Information Security Risk Assessment Questionnaire (CISRAQ). That evaluation holds the most knowledgeable person, usually the business owner or executive sponsor, responsible for gathering the necessary information used to assess the cybersecurity risk of the initiative. Prior to implementation, IT evaluates, tests, and approves all new technology requests, including proposed hardware, software, and/or configurations for consistency with established internal standards to ensure proper support, back-up and recovery infrastructure, and compatibility with other existing technology. In addition, if the initiative includes a 3rd party who will store, process, or transmit Eversource, non-public information, then a Due Diligence Questionnaire (DDQ) must be completed. This document describes the internal security controls used by the 3rd party to protect the data (Technical and Customer/Employee Personal data) being provided. If the controls are deemed not acceptable, then changes must be made or the data will not be authorized for release.

In addition to shared best industry (cyber and utility) security practices, Eversource is in full compliance (through their audited programs) with NERC CIP standards, FTC Red Flag Rules, Federal Code of Fair Information Practices for Customer Privacy, HIPAA rules, HITECH rules, Sarbanes Oxley rules, SEC rules.

Planning, design, and implementation of all cybersecurity infrastructure, practices, procedures, and so on are based upon the above-referenced standards and practices. In its deployment processes, Eversource applies leading cybersecurity principles, including a *defense-in-depth* strategy. The approach uses layers of different, but complementary *best of breed* security technology to augment Eversource's protection programs. This approach is consistent with the security architecture proposed by DHS: *Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies* (2009), and *DHS Strategy for Security Control Systems* (2009). Eversource's programs include creating security risk zones that segregate risk.

3. Asset, Change, and Configuration Management

Eversource manages the organization's Operational Technology (OT) and IT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives. Eversource IT maintains an asset inventory of all computing systems (Servers, PC, Storage systems, etc) in the IT Connect Configuration Management Data Base (CMDB). IT also records the applications that utilize servers and other devices in this same data base. A discovery service scans the network daily to identify new assets on the network. The server request process also has steps for automatically updating the CMDB. The IT Connect Service Mapping utility determines what systems communicate with other systems. This process helps to determine impacted systems when there is an outage. The third primary asset category is Company Data. Legal manages the Exterro Records and Information Management Data Inventory system. This system survey's the Eversource management team to identify what types of data (Business, Operational, Technical, and Customer/Employee) are used by which department. The system also records where the stored and ultimately what the record retention requirements are. This system is not yet integrated with the IT Connect system, however by using the location information, the servers and applications can be mapped to the CMDB.

Industry best practices are used for asset, change, and configuration management. Distribution control center applications are governed by IT policies for change management (Change Management Policy). That policy is enforced by change management procedures and workflow included in the change management tool called IT Connect. Critical applications are captured in the configuration management database (CMDB).

Tracking methods for modifications or changes to the inventory of distribution system assets, system configurations, vendor and equipment models, and firmware are accomplished using technology platforms and configuration and control processes.

System drawings also reflect security devices when applicable. In addition, there are various IT processes and reviews to ensure protection, including event logs and operational monitoring.

The Change Control & Configuration Management Procedure is used for all change and configuration management requests associated with key IT cyber assets. This procedure is used by all personnel within IT for all systems supported by IT. Changes to key cyber assets are documented with the change management process in ITSM. All changes to critical cyber assets follow best practices of testing any changes in non-production environments. Once the impact of those changes is fully understood, a formal change ticket is created with a description of changes, the window of implementation and approvals, as well as presenting the change at the weekly IT change meeting.

3.1 Critical Asset Identification

As required by NERC CIP standards, formal CIP procedures and plans are maintained to methodically identify those assets deemed critical to the reliability of the bulk electric power system. Those plans and procedures dictate periodic reviews to assess, update, and validate the asset list. A similar assessment is required when substantial changes to the cybersecurity environment occur and/or when new equipment and/or configurations are implemented. Additionally, there are cyber assets within IT, OT, and distribution environments that do not currently fall under the scope of CIP standards but to which Eversource, at its discretion, applies similar criteria and processes to more appropriately protect those assets it deems similarly critical.

4. Identity and Access Management

The objectives of the identity and access management processes are to create and manage identities for entities that can be granted logical or physical access to the organization's assets and control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

4.1 Establish and Maintain Cyber Access

The IT Policy "08 Access Control" describes the requirements for administering computer resources. This policy establishes the process for granting and maintaining access privileges on Eversource's network and all associated computer resources and defines the responsibility and authority for the performance of access activities.

This policy is enforced by the Access Administration Procedure, which describes the access request process and requires use of the IT Service Request System. In addition, "08 Access Control" policy defines the security requirements for IDs and passwords, and in part requires: use of unique identifier technologies such as a unique logon ID for each system user that is driven by a centralized Person Information Database used to track employees and contingent workers; User logon ID's must have strong complex passwords that are secured and not written down; Logon ID's are locked from use after a defined number of failed login attempts; For system accounts, default passwords must be changed periodically; and a Privileged Account Management system is used to limit access. All system access is driven by the *least privilege* principle and an access request must be properly approved before access is granted. Access is authorized only on a *need to know basis*. For remote access and for selected high risk systems, two-factor authentication is required. In addition, a second set of authentication credentials are required where stronger password policies are enforced.

Monitoring of user behavior is performed using various security technologies. Anomalies such as where users log into computing systems with tolerances, unusual login times or methods are monitored with alerting. The Corporate Information Security Team will also consider significant business events for developing new monitoring rules. Examples could include strikes, layoffs, or other possible restructuring events. Additional policies and enhanced Insider Threat monitoring will be discussed with the Governance Committee.

Termination procedures ensure that network and CIP access for terminated employees and contractors is removed upon receipt of notification. Employees receive periodic reminders to record all terminations prior to the effective date. Monitoring is also in place to identify postdated terminations. Specific communications reminding the supervisor and their manager that terminations must be recorded in the HR system prior to the effective date. There is also a *"for cause"* emergency termination process that is used to remove system access immediately. Semi-annually, all logon credentials are reconciled to a Human Resources list of active employees and all contingent workers are confirmed with designated Eversource management. Quarterly or annual access certifications with system owners are conducted based on system type as designated by corporate requirements. In addition, there is a weekly review of terminations and transfers to ensure that access levels have been adjusted or removed on identified systems, as appropriate. Unauthorized access is monitored using special password lock-out procedures and, for selected systems, an alert is generated requiring a review and disposition by the IT Security Department. Internal testing of the access administration process is conducted and overseen by the IT Compliance Department. Also, audits of the access administration activities are conducted by the Internal Audit Department and external auditors, as well as NERC and ISO-NE (Independent System Operators of New England).

4.2 Physical Access Controls for Employees and Vendors

Because the cybersecurity environment includes physical elements (technology, equipment, and so on), it is important to provide some overview of aspects of Eversource's Physical Security Plan in the context of its relevance to cybersecurity. Eversource has extensive experience with physical security programs based on its work required to protect the bulk electric system. This experience includes ensuring that physical locations are protected with physical security perimeters. Access points and measures to control entry have been established. Procedures to monitor physical access have been implemented including the monitoring of card key access and other means. Security personnel are in place to control physical access on-site or at remote monitoring locations on 24 hours a day/7 days a week basis. Alarm systems, physical access logs, and human observation of access points are all methods used to monitor physical access to protect physical locations. Employees who lose their badge are required to report the event to Physical Security.

All new employees undergo thorough background checks before being granted any level of computer system access. Once cleared for employment, individual work needs are evaluated and formally reviewed prior to the employee being given very granular access (that is, access to systems that are in any way sensitive is granted only on a need-to-access basis). Similarly, physical access to areas with cyber sensitive equipment is granted only to those with a specific need. All such areas are card-key controlled with formal procedures for granting and using such access, all of which is recorded and monitored. Areas and systems with higher levels of sensitivity such as CIP areas require additional background checks prior to such access being granted. Procedures for all of these processes cover authentication, verification, tracking, and so on CIP-related processes and procedures are reviewed annually and audited by regulators and third parties every 3 years.

Termination procedures ensure that access for terminated employees and contractors is removed in a scheduled and timely manner. There is also a for cause emergency termination process that is used to remove system access immediately.

Periodic checks and audits are conducted to validate that appropriate access is in place.

5. Threat and Vulnerability Management

The objectives of the threat and vulnerability management processes are to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (for example, critical, IT, operational) and organizational objectives.

The Threat Profile for Eversource Energy considers the various "Threat Actors" who may have intent to attack Eversource Systems and data. These Threat Actors include Cyber Terrorists, Organized Criminals, and Nation States. These Threat Actors may use various forms of malware including, but not limited to, ransomware, Remote Access Trojans, Root Kits, Worms, or Crypto-mining technologies. These Threat Actors intentions when using these tools is to either obtain persistence in the network for future use, disrupt business and operations systems, or compromise technical or customer/employee data.

Eversource uses the following threat information sources to incorporate into all threat monitoring technologies (In Priority Order):

- Department of Homeland Security
- Federal Bureau of Investigation
- Electric Sector Information Sharing and Analysis Center
- US- Center for Emergency Response
- DOE
- Others as necessary

5.1 Existing Systems

CIS applies leading security principles and practices to protect the infrastructure and computer networks from cyber-attacks including a defense-in-depth strategy. Eversource uses *best of breed* specialized security technology is used such as host and network-based firewalls, intrusion detection systems, virus and anti-malware protection, file encryption, content filters and vulnerability scanners to further reduce risk of compromise. This security architecture is consistent with recommendations from DHS's *Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies*.

For deployed systems, periodic reviews and audits are conducted by internal and 3rd parties to ensure the security controls are functioning as designed. In addition, penetration tests and/or vulnerability assessments are conducted to validate the system security controls on a periodic basis.

For control systems, no automatic assessments are performed on production environments due to potential operational impacts by assessment tools. Assessments of control systems are done using manual data collection and analysis. The assessments include gathering intelligence from multiple reliable sources (vendors, ES-ISAC, Edison Electric Institute (EEI), and so on) and implementing response/mitigation plans.

All mobile devices including laptops, tablets, and smartphones must utilize encryption technologies to secure company data.

5.2 New Systems

There are many controls and processes used to validate systems in pre-deployment. CIS begins the security assessment process in the system purchasing phase by including security requirements in the request for proposal (RFP) and scoring security levels in the proposal evaluations. A security risk assessment process known as CISRAQ is required by the Methodology for Project Management. In addition, security approval is required as part of the change management process for any new systems deployed in the IT-supported production environment.

5.3 Outside Services

The IT Security team monitors multiple threat advisory services such as Industrial Control Systems Cyber-Emergency Response Team (ICS-CERT), ES-ISAC, InfraGard, and SANS Internet Storm Center. Eversource also subscribes to a paid advisory service. All alerts are reviewed for applicability and analyzed for impact to the company. When mitigation is not available or cannot be implemented, the compensating measures are reviewed for mitigation effectiveness and to ensure the risk level is low. In these situations, the mitigations are reviewed with system owners. In addition, Eversource has multiple 3rd party forensic service providers that can be utilized if needed for a security event.

5.4 Security Patch Assessment

IT Security performs the assessment of security patches at the Enterprise Patch review meeting that is conducted monthly. Minutes and actions are captured as a result of the monthly patch assessment.

As part of the assessment process, individuals across Eversource who are identified as Subject Matter Experts (SME) for software related to a patch or upgrade provide input into the evaluation, testing, and installation of that software. The assessment process uses the defined CVSS (Common Vulnerability Scoring System) to help quantify risk and potential impact. All applicable devices are required to be patched based on the approved schedule.

Eversource follows the NERC CIP Security requirements where applicable to this area. Real-time systems, communications networks, and interfaces are secured on the host side with firewalls and other industry best practices described in

- NIST Standard 800-82 Guide to Industrial Control System Security
- DHS Industrial Control System Standards

5.5 Security Patch Management

Along with a rigorous IT patch management program for infrastructure and applications, the Security Patch Management process follows standard Change Control and Configuration Management Procedures. This process is used to track, evaluate, test, and implement cybersecurity software patches.

Security patches and upgrades are tested before being installed in production unless there is no development environment. In that case, documentation of the exception and the compensating measures applied to mitigate risk exposure are required.

5.6 Vulnerability Assessment Process

Eversource performs 3rd party vulnerability assessments on an annual basis on selected systems based on risk and compliance requirements. Vulnerability assessments are required by the NERC CIP standards for systems classified as critical. An external third party is selected to conduct the assessment. Eversource has also engaged with the Department of Homeland Security CISA to perform external vulnerability scanning services. The Information security team also periodically scans the internal network for vulnerabilities and monitors remediation.

Eversource performs application vulnerability scans as part of the System Development Life Cycle (SDLC). The scan is performed during final application testing to ensure that no critical security vulnerabilities exist prior to deployment of the application. These scans also occur on major system changes.

Eversource will perform “Red Team/Blue Team” testing which will ensure the preventative cyber technologies are in place and to test the company’s resistance to Social Engineering and the Cyber teams Incident Response procedures.

6. Situational Awareness

The objectives of the situational awareness processes are to establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP). As part of this COP, a Security Operations Center has been established for the monitoring of security events. This team is staffed 24X7, 365 days a year. They will perform the initial risk assessment and triage for the event and escalate to the level 2 support team when needed.

U.S. DHS Daily Open Source Infrastructure Report Updates provide relevant information that is reviewed and forwarded as appropriate to Corporate Security. More urgent/time-sensitive and focused briefings come on an emergent basis from the Department of Energy (DOE), DHS, ES-ISAC (directly to control rooms) and state agencies such as the Connecticut Division of Emergency Management and Homeland Security (CT DEMHS), the Massachusetts Emergency Management Agency (MEMA), and the New Hampshire Division of Homeland Security and Emergency Management (NH HSEM). These updates include classified and unclassified information, depending on the sensitivity of the data. These agencies have alert and text systems for alerts on any type of creditable threat such as weather, earthquakes, amber alerts, or terrorist alerts. They send situational reports and briefings, including weather forecasts and related information. Additional information is included in the Physical Security Plan.

The company's bulk transmission operators in each state share NERC and ISO alerts or actions they receive. Formal operating procedures dictate actions based on those alerts. EEI sends reports or information through the Business Continuity (BC) and Mutual Aid work room accounts to which Emergency Preparedness leadership subscribes. Corporate Security forwards any relevant information from state fusion centers and the FBI to operations control rooms.

IT receives updates of both urgent and less time-sensitive natures on security patches and vulnerabilities from vendors. Rigorous patch management/change management processes ensure that these alerts are triaged and acted upon appropriately.

6.1 Logging

Enterprise security policy requires that logging be enabled where technically possible in order to capture cybersecurity related events of significance. Logs containing cybersecurity related events from key systems are collected in a central logging repository, which is monitored for unauthorized activity. These logs can be used to support the Incident Response process.

6.2 Monitoring Electronic Access

Key network activity is monitored 24/7 by a contracted Managed Services Security Provider (MSSP) that alerts the IT Security team in the event of unexpected or unauthorized activity.

In addition, daily reports are generated by the central logging repository for review by the IT Security team. These reports are based on specific conditions that can indicate a security issue or threat.

Electronic access logs are retained for 12 months. Logs related to reportable incidents are retained for a minimum of three years.

7. Information Sharing and Communications

The objectives of the information sharing, and communications processes are to establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks, and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

7.1 Cybersecurity Threat Information Sharing

Eversource participates in several information sharing communities and has defined processes for when to share threat information. The nature of the information largely determines the frequency with which it is shared. For example, emergent, urgent information with significant potential impact is shared immediately. However, CIS executive management (including the Board of Trustee) are periodically briefed on events and alerts during the year. That briefing includes examples of newsworthy cybersecurity items that were reviewed and either acted upon or documented as not needing action. It provides examples of risk assessment, reviews of any incidents, other current items of interest, and so on.

IT Security monitors multiple external threat advisory services such as ICS-CERT, ES-ISAC, Infragard, and SANS Internet Storm Center. Eversource also subscribes to several paid advisory services. All alerts are reviewed for applicability and analyzed for impact to the company. In addition to the advisory services, IT Security regularly networks with security personnel from other utilities.

Sharing security related information obtained in a security incident is a requirement of the All Hazards Emergency Response Plan and will be done by the Information Security organization. Eversource incident response procedures include steps to engage with the ES-ISAC to share the threat intelligence is part of this procedure. Depending on the situation, other organizations will be included, such as the FBI and DHS.

Communication is a key role in the incident response process and IT Security also engages internal stakeholders as part of the process.

7.2 Information Protection Policy

Information sharing activities are guided by documented policies. Any information that has not been publicly disclosed is protected against improper disclosure, both inside and outside Eversource.

The Records and Information Management Policy governs how Confidential Information (CI) is defined. Types of such information include Confidential Business Information (CBI), Critical Infrastructure Information (CII), information related to Critical Infrastructure Protection (CIP), Critical Energy Infrastructure Information (CEII), Confidential Personal Information (CPI), and Protected Personal Information (PPI). The policy also defines protocols for the treatment of confidential information, Contractor and Third-Party Confidentiality Agreements, and Confidential Data Breach or Loss. 3rd Parties are required by contract to notify Eversource of a data breach. Additional guidance is provided in the Records Retention Schedule and in the Identification, Protection and Labeling of CEII Materials administrative procedure. Compliance to policies is audited periodically by the Internal Audit Department.

7.3 Data Protection

The Cyber Security team utilizes various preventive and detective controls to ensure security of company sensitive information including technical engineering data, Customer and Employee personal data. Preventative tools monitor for sensitive information in motion (unencrypted) or at rest in an unapproved location. The Eversource Data Loss Prevention (DLP) tools monitor various, but not all data repositories across the Eversource network. If PII information is found by these DLP tools, they will block and alert the Security team of an issue.

Eversource performs quarterly access reviews for SOX applications, NERC CIP systems, and in Microsoft Azure. These reviews are intended to ensure only authorized persons have access to sensitive data and systems.

7.4 Data Loss Prevention:

Eversource's IT Security DLP Strategy includes reference to policies, control standards and control procedures which include tools and processes that detect and prevent unauthorized access, misuse, destruction of critical or sensitive data. Policies in place that support this strategy are as follows:

- Data Classification Policy: includes classification categories and the process for associating data to each identified classification and how each shall be managed. The continued development and growth of the process includes identification of mandatory controls for each specific type of data classification, or individual controls for subsets based on the technology allowances as to where the data is maintained for business use or at rest.
- Records Retention Policy: Detailing retention periods by record type, for use by the business owners and users of records.

Technical tools for the areas of focus as noted below, are managed within IT Security as our DLP strategy include, yet are not limited to:

1) **Data Classification** – Eversource has the capabilities to watermark and classify Microsoft Office files in accordance with the Company's Data Classification Policy. All employees are responsible to apply these controls where appropriate.
2) **Unstructured Data** – Utilize Microsoft Rights Management to encrypt sensitive data and to apply controls around printing, copying, saving and granting additional access directly to a file. The technology also can scan and tag files within specific data folders based on policies established. Once files are tagged, they will be protected with default protections that encrypts the files. If files are transmitted in error, or inappropriately, the files will be unavailable to recipient unless proper access is granted via the Microsoft Rights Management rules/policies.
3) **Email** – Technologies include Proofpoint and Microsoft Rights Management (previously known as AIP). Configurable to identify specific filters and alerting capability to prevent data loss – example can reject email transmission with SSNs, bank account formats etc.
4) **Databases** – Technology utilized is Imperva Database Protection. This technology is an agent-based technology installed on databases (currently in place). Alerts on large file export and other database-focused loss/leaks, etc.

8. Event and Incident Response, Continuity of Operations

The objectives of the event and incident response and continuity of operations processes are to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

8.1 Data Breach Program

The Data Breach Readiness Program is a corporate-wide program with representatives from Legal, Corporate Communications, IT Security, and Business Segments as needed. The program includes a dedicated Incident Response Team (IRT) that is assembled upon notification of an incident to the IT Security Team and where the potential of a breach exists. Notification to appropriate IRT members is based on an established IT Incident Response Process including paging and notification. Additionally, Eversource uses a *Personal Information Data Breach Incident Response Manual*, which is reviewed and updated as necessary. This manual includes a policy statement, response team assembly, overview of Cyber Incident structure and process, roles and responsibilities, high-level communications workflow, customer communications, media and investor relations, and legislator and regulator communications protocols.

Data breach plan provides guidance for the management of a significant breach or loss of confidential personal information (Data Breach Incident) requiring notification to impacted persons (customers or employees), potential notification to and involvement of law enforcement and/or other governmental authorities, and communications with regulators and investors. That manual is focused primarily on communications and references other Data Breach Incident response procedures and materials, such as IT Incident Response Procedures, the All Hazards Incident Response Plan (AHP) and business unit activities, which are part of the comprehensive plan for timely management and response to a Data Breach Incident. Communications regarding a Data Breach Incident are managed to comply with laws and to mitigate the negative impact on the relationship between the information owner and the company entrusted with it.

8.2 Business Continuity Plans

Business Continuity Plans are maintained to ensure the ability to continue crucial and critical business processes during and after a disaster (any challenge to the ability to conduct those processes). Business Continuity Plans provide for the loss of people, facilities, and systems related to each covered process. Each plan, integrated with the overall incident response processes, provides specific guidance for continuing a specific critical or crucial business process during and after a disaster.

8.3 Disaster Recovery Plans

Similarly, Eversource maintains IT Disaster Recovery (DR) plans that ensure the ability to recover, in a predetermined and timely manner, technology and associated data after a disaster. DR Plans for all time-critical non-CIP systems are maintained in the IT DR Runbook and are exercised annually. DR plans for CIP-related systems are maintained in classified CIP plans which provide an integrated DR and incident management approach.

8.4 All Hazards Plan

The very nature of a utility includes core business processes for which incident response is a nearly routine occurrence. Leveraging that experience is key to the integration of all types of incident responses in the AHP.

The AHP is established as an overarching framework for the implementation of the comprehensive Emergency Management Program. The AHP provides guidance used to direct operations and staff assignments, procure and allocate resources, and take measures to restore normal services and operations. This overall Emergency Management Program is consistent with the criteria for emergency management and business continuity programs established by National Fire Protection Association (NFPA) 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.

The purpose of the AHP is to provide a framework for identifying, preparing for, and responding to emergency situations and other extraordinary events consistently and effectively. Although not inclusive of every possible emergency situation that might occur, it provides key information regarding emergency and business continuity practices to be utilized system wide. A clear effective response to events ensures the safety of employees and the public and the protection of assets. By providing a comprehensive emergency response plan, the effects from any disruption of service are minimized and the safety of employees and the general public is maintained.

8.5 Eversource All Hazards Emergency Response Plan

Eversource maintains an All Hazards Emergency Response Plan. Supplemental plans that specifically address critical infrastructure are maintained as required by NERC CIP. Criteria to identify security events are listed in these Plans.

IT maintains a separate IT Incident Management process that is used for IT-specific incidents that do not warrant the response level of the All Hazards Incident Management Plan or NERC CIP plans. This process follows similar methodology to the other response plans and is focused on specific IT technology.

Incidents are identified through multiple means of detection including monitored security events. Security events that are detected are reported to the Information Security team. The events are reported through the Enterprise ITSM tool and the details are tracked in a Confidential Investigations Database.

Information Security has established a forensic skillset for collecting data and performing initial analysis. Eversource is also establishing contracts for advanced forensics services with third parties. Forensics activities will be activated during a security incident where there is an unknown cause or the likelihood of engaging law enforcement.

The All Hazards plan also includes a section on Data Incident Response. This plan describes the different types of data (Technical, Operational, Business, Customer/Employee, etc.) incidents, how the response team is to be organized and the responsibilities of the different members. The document also has templates for internal communications regarding the incident and external reporting.

Eversource has implemented a program for managing Distributed Denial of Service (DDoS) attacks. Eversource has a third party that would be activated to filter network traffic related to the attack. Standard procedures describe how this process will be activated and return to normal operations.

8.6 Eversource Ransomware Response Plan

Eversource has implemented a plan for responding to a ransomware attack. This plan addresses the engagement with the adversary, and the process for determining if a ransomware payment should be made. Technical response and remediation of a ransomware attack is included in other response and operational plans.

9. Supply Chain and External Dependencies Management

The objectives of the supply chain and external dependencies management processes are to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent upon external entities, commensurate with the risk to critical infrastructure and organizational objectives.

9.1 Procurement Security Controls

A comprehensive process is used for evaluating risks and helping ensure that vendors do not pose undue risk to the company and its customers. This risk assessment starts with obtaining a Security Score from an independent third-party rating service that is based on the vendor's security controls information. Security scores will be obtained for new vendors providing critical parts or services, as part of the Vendor Certification process. Vendors must have acceptable scores or commit to remediating the identified risks to do business with Eversource. A standard RFP process is used when procuring technology-related solutions. This process requires vendors to respond to requirements related to security capabilities and functional security controls. The cybersecurity procurement language for energy delivery is included in the RFP where possible. Vendors must respond to questions about the technology and demonstrate recognition of NIST ICS security guidelines as well as adherence to NIST security checklist configurations. They must provide baseline security configurations for their products with the ability to enable more advanced security configurations as documented with certifications of appropriate assurance levels of Common Criteria Evaluation. See *Section 2.1, Overall Enterprise Risk Management Program*. Cybersecurity procurement language is included in all contracts, based on what was included in the RFP.

Vendor selection criteria are implemented through four components. The application of these four components as a group for vendor/device selection supports the implementation of enterprise security compliance, policies, and standards as a base capability, and any relevant and specific cybersecurity standards and requirements.

9.2 Compatibility with Existing Equipment within the Enterprise

Hardware, software, and software tools must comply with existing installations. Compatibility is a primary vendor/device selection criterion to ensure systems are fully functional, supported, and can be maintained.

9.3 Adherence to Architecture Standards

Hardware, software, and software tools follow architecture standards. These standards are defined and documented within the IT department, working with internal business partners. The adherence to these standards leverages pre-selected infrastructure, software, and tools that have been selected as leading technologies for implementation.

9.4 Adherence to Standard Procurement Processes

Hardware, software, and software tools are procured through standard procurement procedures that include cybersecurity standards and compliance as part of the vendor evaluation criteria. Additional industry security standards used to create these standards, processes, and procedures are listed at the end of this document.

9.5 Network Security Perimeter and Access Control

Network security supports the "Defense in Depth" strategy by implementing an external security perimeter, multiple internet facing zones for isolating different traffic types, and internal network segmentation. Internal segmentation separates "High Value" zones from the standard corporate network which is used by Eversource employees. The network segmentation strategy will be flexible to allow for changes in risk and a need to segment different business areas.

For vendor equipment or networks not directly under company control, vendors are required to maintain a supervised, secure, controlled, monitored network facility to ensure:

- There are various administrative, technical, and logical controls to ensure that data is secure while resident at the external vendor's network or in transit.
- Industry standard security solutions are deployed to secure data.
- Encryption of data, when appropriate, while resident at vendor's location or while in transit using industry standard encryption and cryptographic methodologies.
- Technology infrastructure that guarantees the availability of information technology assets.
- Access to information technology assets is allowed only by authorized individuals.
- Integrity and privacy of information technology assets is maintained.
- Misuse or loss of information technology assets is prevented.
- Transit of data to/from customer premises is sufficiently secured to guarantee integrity of the data while in transit.

9.6 Vendor Security Program Evaluation

A vendor security review that includes information technology security policies, procedures, and other documents is maintained jointly by CIS and Corporate Security (physical) and is performed periodically. This program requires that vendors perform the following activities:

- Review what is required of them at least annually and make appropriate updates after any significant changes to their business operations, computing, or telecommunications environment.
- Conduct their own information technology security policy review and standards compliance audit at least once every year. That review/audit must be performed by a qualified party or parties, independent of the vendor's information technology organization. The nature and scope of the audit is commensurate with the extent of the vendor's dependence on secure information technology assets to accomplish its critical business functions or as such operations can impact the security of other federal or state organizations.
- Upon completion of the audit, the vendor must enact the recommendations of the audit and the plan for correcting the deficiencies appropriately and provide documented results for review and evidence for final validation.

These measures ensure that vendor selection is made with careful consideration to, and mitigation of, cyber security risks that could potentially be introduced as a result of the proposed vendor relationship and project implementation. Thus, this part of the vendor selection process serves as a key component of the overall approach to cybersecurity. Information Security will also consider all forms of intelligence information as part of the vendor selection process.

In any contract where data is stored off-site, vendors are required to adhere to the IT Security Requirement document. That document is made part of the terms and conditions of any ensuing contract. The vendor is required to complete and return an IT Due Diligence Questionnaire. The information collected on that questionnaire is then processed through the CISRAQ process, with vendor submission evaluations used by IT, Security, the requesting department, and Purchasing to render decisions on the viability of proposals.

Annually, a risk assessment will be performed to identify hardware and service providers that by nature of the products used and services performed, will have the greatest risk to Eversource Operations systems (Relays, transformers, Engineering services, etc.). For the vendors identified through this risk assessment, additional security evaluation will be performed to reasonably ensure products are received in proper form, software is free of malware, and service providers have appropriate controls to prevent unauthorized access to Eversource systems and networks.

10. Workforce Management

The objectives of the workforce management processes are to establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

10.1 IT Security Organization

The IT Security Department is responsible for operating the cybersecurity program for the entire company and resides within the IT organization. This department's mission is to ensure the availability, integrity, and confidentiality of information and systems. They provide consulting services to application development and IT infrastructure teams on security controls enterprise-wide. They manage access for all network users and to selected applications. Additionally, they maintain and operate a variety of specialized security technology that provides protection from external and internal threats.

Job descriptions are provided covering job responsibilities and daily duties for all exempt and non-exempt positions within the IT organization. They cover minimum education and experience requirements for each position and for each level within a position.

In addition to in-house staff, Eversource relies on third-party providers to supply security professionals to perform specific security services.

Training is need-based for each employee, with training funds budgeted through individual development plans. Depending on the subject, availability, or cost, training can be computer or classroom-based and it can be hosted internally or externally. In addition, security staff is encouraged to achieve security certifications.

10.2 Personnel Risk Assessment

Corporate Security administers a program to ensure that only personnel cleared by an appropriate background check are granted cyber or unescorted physical access to defined critical cyber asset. A personnel risk assessment (PRA) with specific predefined criteria is initiated prior to personnel being granted cyber access or unescorted physical access to key cyber assets or information associated with key cyber assets. All personnel risk assessment records are maintained by Corporate Security.

Eversource monitors for inappropriate behavior and implements discipline when appropriate. Violations of cybersecurity policies are tracked (for example number of violations, types of violations, etc.) and end computer users are provided immediate feedback for even low-level violations, such as inadvertently attempting to access a blocked internet website. System monitoring is performed through a tiered approach that uses a specialized external service provider for generic threat protection, and internal monitoring for specific threat protection. Eversource uses a progressive disciplinary process defined by Human Resources, which can include immediate termination based upon the severity of the policy violation.

10.3 Awareness Program and Training

IT Security maintains an enterprise security awareness program that communicates various security measures through a Cyber and Physical Security webpage, the daily company newsletter, posters and email campaigns. Various security messages are sent out quarterly at minimum. Communication is also sent for high profile security news items that impact the company.

Policies and procedures are periodically reinforced through online computer based training and other awareness mechanisms such as posters, management briefings, direct e-mails, read and sign processes, and company newsletters. Newly hired employees are required to complete an online cybersecurity training program. In addition, other departments that are considered high risk such as Human Resources, Customer Service, and System Operations Centers conduct additional specialized cyber security training. Everyone in the IT organization is required to sign a confidentiality agreement annually. Ongoing awareness campaigns include posters, articles in Eversource newsletters, slogans (such as *Human Firewall* and so on), policy links and other occasional item-specific informational communications. A quarterly committee meeting plans CIP-related security awareness effort, which include non-CIP specific campaign content as well.

11. Cybersecurity Program Management

The objectives of the cybersecurity program management processes are to establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

11.1 Standards Based Security Program

Eversource's cybersecurity program uses existing experience with and knowledge of the CIP framework as the basis for relevant cybersecurity planning. The program also introduces other complementary approaches (for example, NIST 800-30, NIST 800-53, NIST 800-82, NIST 800-171, and so on) where applicable. These guidelines provide a well-defined and understood cybersecurity posture capable of addressing challenges and/or compromises related to the loss of integrity, availability, and confidentiality. IT Security personnel monitor emerging standards by participation in industry standard groups, and are fully committed to identifying, managing, and mitigating cyber security risks.

Annual goals are set for the year to improve the cybersecurity program. These goals help work towards the strategy to constantly improve the program by addressing gaps, meeting new compliance requirements, and implementing new security tools to meet emerging threats and risks.

11.2 Cyber Security Risks and Mitigation

For its bulk electric power systems, Eversource is required to comply with NERC CIP standards for cybersecurity infrastructure and processes. Required tri-annual third-party audits have consistently confirmed the approach to exceeding those standards. That experience and approach is leveraged for all of the cybersecurity processes and infrastructure.

11.3 CIS Governance

Governance, including organization, accountability, policies, processes, and metrics, is based on industry best practices as well as the need to build in agility and the ability to respond to environmental changes, emergent threats and incidents in a timely manner. Organizationally, CIS resides within the IT Department. To facilitate IT's role as a strategic business partner above and beyond its role as a technology service provider, IT is led by a Chief Information Officer (CIO) who is a Senior Vice President. Emergency Preparedness (EP), which leads corporate incident response and disaster recovery processes, is also led by a Vice President within the core business functions of the company. This partnership between CIS and EP permits CIS to respond swiftly and appropriately to cybersecurity incidents by maintaining its focus on the key elements of the cybersecurity response and EP assists in managing and responding to broader issues affecting services or processes that can be involved in a cybersecurity incident. Similarly, EP leverages its extensive utility-based response infrastructure for properly managing all non-IT-technical aspects of a cyber-security incident.

In addition, cybersecurity is discussed periodically at the highest levels of the organization. It is listed as one of the top risks to the organization through the Enterprise Risk Management process and is discussed and reviewed with the Board of Directors as well as the senior executives, including the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, EVP of Human Resources, EVP of Customer Experience and Energy Strategy and the General Counsel periodically throughout the year.

CIS is responsible for operating the cybersecurity program for the entire Company and resides within the IT organization. This department's mission is to ensure the availability, integrity and confidentiality of information and systems. They provide consulting services to application development and IT infrastructure teams on security controls enterprise-wide. They manage access for all network users and of selected applications. Additionally, they maintain and operate a variety of specialized security technology that provides protection from external and internal threats.

11.4 IT Security Organization

The IT security organization has one Vice President – Chief Information Security Officer, reporting to the CIO, responsible for all aspects of information security and compliance. Reporting to the VP – CISO is a Director – Information Security focused on security operations and architecture, a Manager for Compliance and Identity, Manager for Network, and Manager for Artificial Intelligence. Reporting to the Director – Information Security is a Manager focused on Operational Security Technologies, Manager of Corporate Security Technologies and Incident Response, and a Manager focused on Security Architecture.

IT security professionals hold a variety of certifications and attend annual training and conferences to stay abreast of the security landscape.

A variety of outside services to complement internal skills and capabilities are also employed. Some IT Security outside services being used today include 24x7 monitoring of intrusion detection and firewall technologies, computer forensics and penetration testing/vulnerability assessments.

IT Security also meets with the IT Business Unit Leads, the Governance Council, and various departments to communicate Cyber priorities, projects and areas that need attention from these groups. This helps to ensure alignment with the business, IT and cyber focus.

11.5 Architecture to Protect Critical Systems: Defense in Depth

A layered defense approach features Virtual Private Network (VPN) architecture including firewall segments for each location over the corporate network with strict firewall rule sets that are monitored for unauthorized activity 24/7 by a third party. The Critical Cyber Assets run anti-virus software and are monitored for security related events. Hardened operating systems are used for servers and workstations.

11.6 Architecture to Protect Critical Systems: Boundary Defense/Electronic Security Perimeter

Boundaries are established to define an Electronic Security Perimeter (ESP) around the most critical systems. ESP documentation includes all access points to the perimeters, all key cyber assets within the ESPs and all systems used to control and monitor these access points. The ESPs typically include an intrusion detection layer and firewall layer.

Electronic access into the ESP is implemented through access control lists and firewall rules. Dial-up access is not permitted into the Electronic Security Perimeters. Only ports and services required for operations are allowed across the access point. The access lists are documented and maintained.

Requests for remote access to critical systems are accomplished by way of a formal request and approval process. Once provided, connections are secured through VPN and multi-factor authentication.

11.7 Architecture to Protect Critical Systems: Malicious Software Prevention

Anti-Virus and Malware Prevention Tools and Log Monitoring tools are maintained on cyber assets where technically and operationally feasible. A process for updating anti-virus and malware prevention signatures for malicious software prevention is used.

11.8 Account Management

Procedures are maintained to manage application account provisioning and de-provisioning processes as defined in the Access Administration Policy. Application user access and authorization rights and access privileges are reviewed periodically by the application request approver. Historical audit trails of individual user account access activity are retained.

11.8.1 Security Monitoring

Critical networks are monitored 24/7 by a contracted Managed Services Security provider (MSSP), which alerts the IT Security team in the event of unexpected or unauthorized activity.

The process of monitoring security events for all key cyber assets is documented by way of a security status monitoring procedure that employs multiple processes for viewing and alerting of security events of all key cyber assets within the Electronic Security Perimeter. These methods include manual viewing of firewall logs, servers, workstations, and IDS Event log analysis. Electronic access logs are retained for six months. Logs related to reportable incidents, are retained for a minimum of three years.

11.9 Cyber Vulnerability Assessment

Ongoing and continuous threat/vulnerability assessments include gathering intelligence from multiple reliable sources (vendors, ES-ISAC, EEI, and so on) and implements response/mitigation plans. An annual vulnerability assessment is conducted on the NERC CIP defined systems.

11.10 Disposal or Redeployment

A formal disposal and redeployment process ensure that all key cyber assets and associated data storage media within the existing Electronic Security Perimeter are properly handled to ensure that no sensitive data can be retrieved. Such disposals employ best practice erasure procedures prior to physical disposal of media.

11.11 Cybersecurity Plan Updates

The cybersecurity plan is reviewed and updated on an annual basis to address new or changed vulnerabilities. A revised cybersecurity plan is published annually and after off-cycle changes.

12. RECORD OF CHANGES

Revision 0

Revision 0 was developed in the Spring of 2015 as a collaborative effort led by IT and EP leadership team.

Revision 1

Revision 1 was performed in Fall 2015 and was specifically performed to modify the format of the document to comply with the Eversource Emergency Management Program documentation requirements. Additionally:

- The Revision Change page was moved for the front of the document to Section 12.
- The original section “Overview and Cyber Security Approach,” and section “Document Purpose” were switched in order of presentation.
- Original section “Organization of Cybersecurity Plan Elements,” was removed and replaced with a formal Table of Contents inserted at the beginning of this revision.
- Some terminology was modified to reflect the rebranding of the company to Eversource Energy.
- The of Acronyms List and the References List were converted to Attachments 1 and 2 respectively.

Revision 2

- Revision 2 expanded the Risk Assessment process to include the Cybersecurity Risk Assessment process. In addition, changes to the Vulnerability Assessment section were made to add new assessments.

Revision 3, effective 6/25/19

- Updated section 4.1 to add details on access controls and to update the reference to the Access Control policy
- Updated section 5.1 to add information regarding encryption on mobile devices
- Updated portions of section 9 to address vendor risk management

Revision 4, effective 7/6/20

- Minor grammatical edits

Revision 5, effective 4/13/21

- Minor edits for currency
- Added Data Protection section

Revision 6, effective 12/10/21

- Updated Section 5.6, Vulnerability Management to include Red Team/Blue Team testing.
- Updated Section 7 to add 7.4 regarding Data Loss Prevention

Revision 7, effective 11/30/22

- Minor edits for currency

Revision 8, Effective 12/15/23

- Updated IT Service Management system for assets to IT Connect
- Added Department of Homeland Security vulnerability Scanning to section 5.6 Vulnerability Assessment Services
- Added section 8.6 Eversource Ransomware Response Plan

Revision 9, Effective 12/19/2024

- Updated for minor grammatical updates
- Updated cyber organization structure

Attachment 1
Acronyms and Abbreviations

(Sheet 1 of 1)

AHP: All Hazards Plan – integrated incident management/response plans

BC: Business Continuity

BIA: Business Impact Analysis

CBT: Computer-Based Training

CIP: Critical Infrastructure Protection, NERC standard

CIS: Eversource Corporate Information Security department

CISRAQ: Corporate Information Security Risk Assessment Questionnaire

DHS: United States Department of Homeland Security

DR: Disaster Recovery (usually meaning IT Disaster Recovery)

ERM: Enterprise Risk Management

ESP: Electronic Security Perimeters

ICS: Industrial Control Systems (NIST)

IDS/IPS: Intrusion Detection / Prevention systems

ITSM: Information Technology Service Management system (help desk trouble ticket tracking, and so on)

IP: Internet Protocol

IT: Information Technology

NERC: North American Electric Reliability Corporation

NIST: National Institute of Standards and Technology

OT: Operational Technology

RFP: Request for Proposal

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SOX: Sarbanes Oxley Act of 2002

Attachment 2
Reference Documents

(Sheet 1 of 1)

These documents were used in creating standards, procedures, programs for cybersecurity

- NIST Special Publication (SP) 800-53 — Recommended Security Controls for Federal Information Systems and Organizations.
- NIST Special Publication (SP) 800-30 — Risk Management Guide for Information Technology Systems.
- NIST Special Publication (SP) 800-82 — Guide to Industrial Control Systems (ICS) Security.
- ISO 27002 — Information technology – Security techniques – Code of practice for information security management.
- OpenHAN — Home Area Network (HAN) device communication, measurement, and control.
- IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.
- Security Profile for Advanced Metering Infrastructure, v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009.
- IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security.
- NIST 800-92 - Guide to Computer Security Log Management – EVERSOURCE leverages this guide when the opportunity presents itself to select and implement a SEIM technology.
- Cybersecurity Capability Maturity Model (February 2014) http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (Note: This model was used as a means to organize cybersecurity attributes within the Eversource Cybersecurity Plan, including the objectives listed throughout the plan. The model focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate.)