1.0 PURPOSE

1.1 To reduce the vulnerability of cyber-attack, specific requirements for cyber-security administration, monitoring, protection, and oversight are applied to cyber assets within electric generating facilities.

1.2 This policy implements cyber-security requirements of the NERC Critical Infrastructure Protection (CIP) reliability and compliance program, standard CIP-003-8, "Cyber-Security – Security Management Controls" applicable to facilities designated at the low impact level. In addition, selected principles as recommended by the National Institute of Standards and Technology (NIST) are included, such as: isolation of mission-critical systems from public access; a clear delineation of logical security boundaries; use of a protected, layered architecture; least privilege access control, information protection, and operation under the assumption that any external network connection is insecure.

1.3 This document does not supersede any of the Xcel Energy corporate policies. The intent of this policy is to expand upon those expectations and address them on an Energy Supply level. In the event that an issue is not addressed in this document, the Enterprise Information Security and Technology Standards should be consulted.

2.0 APPLICABILITY

2.1 This policy applies to all Xcel Energy Bulk Electric System (BES) generating facilities that meet the following conditions:

2.1.1 Are identified as CIP regulated at the low impact level under the corporate program for BES Cyber System Identification and Categorization [CIP-002-5.1a] as shown in Attachment 1.

2.1.2 Contain BES Cyber Systems (BCSs) that provide named reliability operating services. For Energy Supply, these services are in the following categories: Dynamic Response to BES conditions; Controlling Frequency; Controlling Voltage; Monitoring and Control; Restoration of the BES; and Situational Awareness [CIP-002-5.1a].

2.1.3 Utilizes microprocessor-based data acquisition systems that collect or store potentially sensitive or proprietary information. This includes but is not limited to unit and equipment operating status, production and consumption rates and environmental data.

2.2 Facilities regulated by the U.S. Nuclear Regulatory Commission are exempt from this policy.

3.0 RESPONSIBILITIES

3.1 The Manager of Fleet Engineering is responsible for designating a Regional System Administrator for each operating region (SPS, PSCo, and NSP).

3.2 Plant Network Delegates

3.2.1 Complete the Plant Network Inspection Checklist in compliance with this policy, and coordinate responses and approval with Regional System Administrators.

3.2.2 Assist with local network issues

3.3 Regional System Administrators

3.3.1 Develop, maintain, and document a Plant Network Security Plan and review with Plant Network Delegates

3.3.2 Limit BCS access to those staff who need access to perform their jobs; the type and level granted shall be the minimum level required to perform the assigned work. Username and Password authentication shall be used for all access to any device on a BCS plant network. For these systems, the default manufacturer’s password shall be changed to unique and strong passwords, where technically feasible. If a unique login is not technically feasible or will prevent an individual from being able to perform their job responsibilities in a reasonable manner a documented exception will be required.

3.3.3 Firewall administration, including final approval and implementation of rule sets and changes to them, as justified by business need.

3.3.4 Documenting the business justification and approval for rules not being logged or turned off

3.3.5 Compliance review and approval of the Plant Network Security Plan and Plant Network Inspection Checklist every 15 months.

- This is done by reviewing the Plant Network Security Plan and Plant Network Inspection Checklist and moving them to the “released” state in ProjectWise

3.3.6 Investigation and disposition of suspected cyber-security incidents, notification of the Enterprise Command Center (ECC) if indicated and submitting required forms in SharePoint.

3.3.7 Logical access to each plant BCS network shall be managed by the Regional System Administrator, who shall review and approve the rule change form submitted by the Plant Network Delegate where applicable.

3.4 Energy Supply CIP Senior Consultant is responsible for:

3.4.1 Review and update of this policy as necessary or at a minimum every 15 calendar months.

3.4.2 Update e-Learning course: “Plant Network Security Policies” as necessary or at a minimum every 15 months

3.4.3 Review administrator access for Regional System Administrators as necessary or at a minimum every 15 months

3.4.4 Administration of storage repositories

3.4.5 Updating and maintaining SharePoint Processes

- Energy Supply Firewall Change Request Form and Workflow
- Energy Supply Smart Key Request Form and Workflow

3.5 Plant Managers and Directors are responsible to provide equipment, software, and facility resources as needed to support requirements of this policy.

3.6 Plant improvement projects Project Initiators are responsible to plan for cyber-security compliance at the project initiation stage and incorporate cyber-security implementation tasks required to comply with this policy into the project cost and schedule prior to funding and approval. Project planning for cyber-security shall employ the Enterprise Project Management (EPM) system, in accordance with policy “Screening of Projects for Impact on NERC Compliance Program (XES 7.405)”.

4.0 CIP-003-8 REQUIREMENTS

4.1 **Requirement - Cyber Security Awareness**: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

4.2 Energy Supply’s Cyber Security Awareness Program

4.2.1 In accordance with “XEL-PRO-CIP Training and Awareness Program” all Xcel Energy employees and contractors are required to compete the Enterprise Security Awareness course (LPN L0015C-008)

- The Enterprise Security Awareness course covers the four areas that make up Enterprise Security: Cyber Security, Physical Security, Enterprise Resilience and Security Governance and Risk Services. It includes scenarios that cover the security habits that are the responsibility of every Xcel Energy employee and contractor.

4.2.2 In addition to the Enterprise e-Learning course Energy Supply has a supplemental e-Learning course: Energy Supply Cyber Security Policies (LPN R4835C-002) that identifies policies specific to energy supply and reinforces cyber security awareness principles.

- All Regional Systems Administrators, Plant Network Delegates, and their management supporting execution of this policy shall maintain current completion status.

4.3 **Requirement - Physical Security Controls**: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

4.4 **Energy Supply's Physical Security Program**

4.4.1 Adherence to the "XEL-PRO-CIP Physical Security of Low Impact BES Cyber Systems" policy is required to ensure adequate physical security at BES plants.

4.4.2 XES 4.200 Power Plant Physical Security Policy addresses escorting requirements and expectations.

4.4.3 XES 4.210 Electronic Lock & Key Policy requires that electronic locks and keys have been implemented at all the plant physical security perimeters as well as substations and other critical areas.

4.5 **Requirement - Electronic Access Controls**: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

4.5.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

- ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
- iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR61850-90-5 R-GOOSE).

4.5.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

4.6 Energy Supply's Electronic Access Controls Program

4.6.1 Electronic Access Controls are addressed in EPR 4.200P01 Energy Supply Electronic Access Controls Procedure

4.6.2 Use of dial-up connections to plant networks is strictly prohibited

4.7 **Requirement 1.2.4 - Cyber-Security Incident Response:** Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.7.1 Identification, classification, and response to Cyber Security Incidents;

4.7.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.7.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.7.4 Incident handling for Cyber Security Incidents;

4.7.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.7.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

4.8 Energy Supply's Cyber-Security Incident Response Program

4.8.1 All suspected cyber-security incidents shall be reported to the Regional System Administrators or delegate immediately upon suspicion of anomalous activity.

Anomalous activity is that which remains unexplained after normal plant investigation, and includes the unexpected:

- loss of execution of system functions;
- loss of network connections;
- detection of new, unauthorized external connections;
- unauthorized system access,
- antivirus / malware alerts; or
- general abnormal activity.

4.8.2 The Cyber Security Incident Investigation and Reporting Procedure should be reference when dealing with a cyber security incident.

4.8.3 If the cyber incident is suspected to be of malicious intent, and not the result of an error or equipment failure, the Regional Systems Administrator shall engage the Enterprise Command Center (ECC) 612-370-3700 and lead or assist in the subsequent investigation and mitigating actions. Incident responses shall be documented using the "XEL-FRM-Cyber Security Incident Investigation Form" and uploaded to the Cyber Incident Response SharePoint Site.

4.8.4 Energy Supply shall participate in a cyber-security incident response drill at least once every 36 calendar months as led by the involved corporate team.

- Energy Supply participates in GridEx every other year
- In years where GridEx is not scheduled a tabletop drill with the ECC takes place
- Lessons learned will be documented and if response is needed will be assigned a priority and be addressed within 180 days

4.9 Requirement 1.2.5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

4.9.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

4.9.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any: Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

4.9.3 For any method used pursuant to above, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

4.9.4 For Removable Media, the use of each of the following:

- Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

- Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

4.10 Energy Supply's Transient Cyber Asset & Removable Media Program

4.10.1 XES 4.220 Transient Cyber Asset & Removable Media Policy should be referenced when considering the use of Transient Cyber Assets and Removable Media.

4.11 **Requirement 1.2.6 - Declaring and responding to CIP Exceptional Circumstances**

4.11.1 Processes to invoke special procedures in the event of a CIP Exceptional Circumstance

4.11.2 Processes to allow for exceptions to policy that do not violate CIP requirements

4.12 Energy Supply's CIP Exceptional Circumstances Program:

4.12.1 Energy Supply follows the XEL-PRO-CIP Exceptional Circumstances procedure to review and document situations that may warrant suspension or delay in implementing certain compliance requirements as allowed by CIP standards.

4.13 **Requirement 2 - Cyber Security Plan:**

4.13.1 Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in CIP-003-8 Attachment 1.

4.14 **Energy Supply's Cyber Security Plan Program:**

4.14.1 Adherence to the enterprise XEL-POL-CIP Cyber Security Policy. Energy Supply follows the enterprise document and corporate cyber security plan.

4.14.2 In addition to the corporate cyber security plan, Energy Supply maintains Plant Network Security Plans

- Details of these plans and contents can be found in EPR 4.200P01 Electronic Access Controls Procedure

4.15 **Requirement 3 – CIP Senior Manager:** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

4.15.1 The CIP Senior Manager is Jamey Sample and evidence is on file XEL-EVD-CIP Senior Manager Communication

4.16 **Requirement 4 – CIP Senior Manager Approval Delegation:** The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

4.16.1 Adherence to the XEL-PRO-CIP Delegation of Authority Procedure will be observed for the Delegation of Authority for Energy Supply

- Evidence of delegation can be found in XEL-FRM-CIP-Delegation of Authority.docx

5.0 Additional Security Practices

5.1 Internal Connectivity: Plant control networks containing cyber assets with generation capacity that exceeds 1500 MW in a single interconnection will be evaluated for a higher classification. Reasonable effort is made in order to maintain a low classification including but not limited to sectionalizing.

5.2 Remote Station Control: plant control networks shall not control more than one other BES facility, remote from the facility. Remote plant controls shall be isolated from the host plant network.

5.3 Operating System and Application Whitelisting: BCS servers should be configured so that only those programs that are needed for operation and are trusted are installed.

5.4 Operating Systems, Applications and Hardware: Plant networks should have supported operating systems and software that is supported by the involved manufacturers to provide current antivirus and malware signatures and operational patches. A plant improvement project request should be submitted using the project request system if any plant network equipment is no longer supported by the vendor and requires upgrade in order to maintain current cyber-security protections.

5.5 Patch Management and virus/malware definitions: Regional System Administrators or delegate shall update patch and virus/malware definitions for BCS networks, in accordance with instructions provided by systems vendors. A description of patch activity completed each year and reference to instructions used for BCS patches shall be documented per the EPR 4.200A03 Plant Network Inspection Checklist. If virus and patch updates cannot be maintained on a current basis, exceptions shall be documented with justification on the inspection checklist.

5.6 Information Security: All outputs of this policy (Plant Network Security Plan, inspection checklists, suspected cyber-security incident response form, firewall ruleset changes) shall be controlled in accordance with the corporate program for Confidential and Confidential Restricted Information Protection.

5.7 Password Storage: Username and passwords for BES Cyber Assets should be documented and stored in central secure repository. Examples include:

5.7.1 Physical documentation and stored in a secure location

5.7.2 Electronic documentation – stored in a locked file in ProjectWise CIP repository

6.0 RECORDS

6.1 An EPR 4.200A01 Plant Network Security Plan, will be stored in the corresponding Plant's "EPR-4.200 Plant Security Plan" ProjectWise folder.

6.2 EPR 4.200A02 Access Control Process Form will be stored in SharePoint with the corresponding completed form and approval records.

6.3 An EPR 4.200A03 Plant Network Inspection Checklist, will be stored in the corresponding Plant's "EPR-4.200 Plant Security Plan" ProjectWise folder.

6.4 If a plant does not have routable connectivity, an EPR 4.200A04 Non-routable Connectivity Attestation Form must be completed and uploaded into the corresponding Plant's "EPR-4.200 Plant Security Plan" ProjectWise folder and moved into the "released" state

6.5 Electronic Key Requests Forms and approvals are stored in SharePoint

6.6 XEL-FRM-Cyber Security Incident Investigation Form" should be uploaded to the Cyber Incident Response SharePoint Site.

6.7 List of BES Plant & Plant Network Delegates - Live list can be found on Energy Supply NERC CIP SharePoint Site – "Plant Network Contact List

6.8 Version History: Retired versions of documents (This Policy, Plant Network Security Plans, Plant Network Inspection Checklist, etc.) will be filed in an “Archive” folder in the same repository application the current document resides.

7.0 DEFINITIONS

7.1 **Bulk Electric System (BES) Generators:** All units connected to the grid at 100kv or greater and have a gross nameplate rating greater than 20Mva; and dispersed generation facilities with multiple units that have an aggregate gross nameplate rating greater than 75Mva connected to a common bus and connected to the grid at greater than 100 kV. In depth BES definition with inclusion and exclusions can be found on the NERC website.

7.2 **National Institute of Standards and Technology (NIST) Cyber-Security Guides:** Engineering Principles for Information Technology Security, NIST Special Publication 800-27; NIST Special Publication 800-82, Guide to Industrial Control Systems Security; and NIST-Guidelines on Firewalls and Firewall Policy.

7.3 **BES Cyber Assets (BCAs):** Programmable electronic devices essential to the reliable operation of a BES plant, including the hardware, software, and data in those devices. A BCA is a device that if rendered unavailable, degraded or misused, would create a generation outage or de-rate within 15 minutes.

7.4 **Low Impact BES CIP Assets:** In general, facilities larger than 20MVA and less than 1500MW. More detailed information on inclusions and exclusions can be found in CIP-002-5.1a Cyber Security — BES Cyber System Categorization

7.5 **Cyber-Security Incident:** Any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter, or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. [NERC Glossary]

7.6 **Transient Cyber Asset (TCA):** a cyber asset that is: capable of transmitting or transferring executable code, not included in a BES Cyber System, and directly connected (e.g. using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset

7.7 **Removable Media:** storage media that: are not Cyber Assets, are capable of transferring executable code, can be used to store, copy, move or access date, and are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset.

7.8 **Regional System Administrator:** The Fleet Engineering lead for network security monitoring and technical support assigned in each of the three Xcel operating regions: NSP, PSCo, and SPS.

8.0 REVISION HISTORY

Date	Revision	Change
04/12/2013	1.0	Original Issue Supersedes ESO 4.200 to align accountabilities with re-organization. Included best practice security requirements from various sources, including FERC Order and NIST, in preparation step to begin alignment with expected future cyber-security requirements. Detailed requirements moved from this policy to supporting plant cyber-security plan template EPR 4.200_A01.
04/27/2015	1.1	Implementation phase is complete. Deleted note regarding implementation plan in section 1.2. Deleted section 5.0 ‘Implementation Plan’ in its entirety.
09/29/2015	2.0	Updated formatting to comply with XES 1.100P01 Configuration Management for ES Policies and Procedures. Sections re-ordered to improve readability. Revision to align with CIP version 6 requirements and/or Internal Audit Observations as follows: • Revised EPR 4.200A01 Plant Network Cyber-Security Plan Template to document system access and type as required in new NERC terms of LERCs, LEAPs, and BROS; • Added EPR 4.200A02 ES Firewall Rule Change Request to document Energy Supply firewall rule changes; • Added EPR 4.200A03 Annual Plant Network Cyber-Security Inspection Checklist to document patch management instructions and activities; • Added EPR 4.200A04 Energy Supply Cyber-Security Incident Response Checklist to document potential cyber-security incidents and notification of required parties if indicated; and • Added EPR 4.200A05 Modem Session Log to document modem sessions. • Updated definition section to align with NERC terms.

Date	Revision	Change
04/11/2017	3.0	• Minor clarifications for accuracy to NERC Standard verbiage. • Changed Annual references to 15 calendar months. • Removed reference to Work Orders in section 4.11 due to move from SAP to Maximo. Added reference to corporate Physical Security Policy and Corporate Awareness Program. Updated formatting to comply with XES 1.100P01 Configuration Management for ES Policies and Procedures. Sections re-ordered to improve readability. Revision to align with CIP version 6 requirements and/or Internal Audit Observations as follows: • Revised EPR 4.200A01 Plant Network Cyber-Security Plan Template to document system access and type as required in new NERC terms of LERCs, LEAPs, and BROS; • Added EPR 4.200A02 ES Firewall Rule Change Request to document Energy Supply firewall rule changes; • Added EPR 4.200A03 Annual Plant Network Cyber-Security Inspection Checklist to document patch management instructions and activities; • Added EPR 4.200A04 Energy Supply Cyber-Security Incident Response Checklist to document potential cyber-security incidents and notification of required parties if indicated; and • Added EPR 4.200A05 Modem Session Log to document modem sessions. • Updated definition section to align with NERC terms.
07/03/2018	4.0	• Revisions to address the new NERC Standard version CIP-003-7. • Removed LERC and LEAP references and definitions, as they are no longer NERC defined terms. • Modified or removed references as necessary to how they are actually being completed. • Updated SOC to Cyber Defense Center • Removed language relating to dial-up and modem commitments • Updated Architecture Diagram • Minor clarifications for accuracy to NERC Standard verbiage. • Changed Annual references to 15 calendar months. • Removed reference to Work Orders in section 4.11 due to move from SAP to Maximo. • Added reference to corporate Physical Security Policy and Corporate Awareness Program.
10/10/2019	5.0	• Updated all CIP version references to CIP 003-8 • Updated architecture of document to capture all responsibilities in one section • Updated CIP requirement for clarity as to what the requirements are and what process is in place to meet these requirements • Added section on Transient Cyber Assets and removable media
2/26/2020	5.1	• Added to Section 4.4 following GridEx about SOC incident number • Added references to XES 4.210 Electronic Lock & Key Policy (Section 4.2) and XES 4.220 Transient Cyber Asset and Removable Media Policy (Section 4.5) • Replaced “Exception Form” with “Authorization Form” • Added Attachment 1 – Plant Designee list • Moved document repository references into new Section 8.0 and update all links
1/4/2022	6.0	• Created EPR 4.200P01 Electronic Access Controls • Updated references of the CDC to the ECC • Updated Cyber Security Incident Response to follow ECC procedure and form • Updated Attachments and numbers to reflect the use of SharePoint Forms and workflows