21 W CHURCH ST.
JACKSONVILLE, FL 32202-3155
www.JEA.com

Table of Contents

1.0 POLICY STATEMENT 2

1.1 Scope 2

1.2 Definitions 3

1.3 CIP Exceptional Circumstances 4

1.4 Emergency Situations 4

1.5 Accessibility 5

1.6 Enforcement 5

1.7 Retention 5

1.8 Review and Approval 5

2.0 BES Cyber System Identification 6

3.0 Low BES Cyber System Protection 7

4.0 Personnel and Training 8

5.0 Electronic Security Perimeter(s) and Electronic Access Points 11

6.0 Physical Security of BES Cyber Systems 12

7.0 Systems Security Management 14

8.0 Incident Reporting and Response Planning 16

9.0 Recovery Plans for BES Cyber Systems 17

10.0 Configuration Change Management and Vulnerability Assessments 18

11.0 Cyber Asset Information Protection 22

12.0 Appendix A: CIP Senior Manager Assignment 23

13.0 Appendix B: CIP Senior Manager Delegated Authority List 24

14.0 Appendix C: Relation Critical Infrastructure Responsibility Matrix 25

15.0 Appendix D: Designated Access Authorization Authority 26

16.0 Policy & Appendix Revision History (for MD 202 Cyber Security Policy) 28

MANAGEMENT DIRECTIVE: **MD-202 CYBER SECURITY POLICY**

TITLE: **CYBER SECURITY POLICY**

JEA Board Policy Statement on Electric Compliance
"It is the policy of JEA to proactively comply with all applicable FERC, FRCC, NERC and Florida PSC rules and regulations relating to electric system reliability, electric system transmission operations and electric market rules. The Board of JEA hereby directs the CEO to initiate and maintain a formal program which documents and ensures this compliance both in letter and in spirit."

Approved by the JEA Board of Directors

5-15-07

1.0 POLICY STATEMENT

JEA will operate its information systems to adequately protect the confidentiality, availability and integrity of its information systems and the data contained therein. The normal operation of these systems will comply with all applicable federal and state regulations. JEA's Board of Directors has issued a policy statement dated May 15, 2007, on Electric Compliance directing JEA's management to develop programs to support compliance with both the spirit and the letter of applicable Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), Florida Reliability Coordinating Council (FRCC), and Florida State Statutes, rules and regulations. The Board of Directors also approved an Enterprise Risk and Compliance Policy and an Electric Compliance Policy which assigns responsibility for compliance to the Chief Executive Officer (CEO) and provides the corporate structure under which a corporate compliance program operates.

This policy represents management's commitment and ability to secure its CIP Cyber Assets (CCA). Specifically, all covered information systems will be acquired, managed, maintained and retired in compliance with the requirements contained in the North American Electric Reliability Corporation Critical Infrastructure Protection standards (CIP-002 through CIP-014). Additionally, subsets of detailed procedures that represent JEA's compliance to the standards are listed in Appendix C that are utilized to implements the security requirements specified in this policy.

1.1 Scope

This policy applies to JEA employees, contractors and service vendors, with the business need for authorized cyber or authorized unescorted physical access to CCA and/or information that controls or could impact the reliability of the Bulk Electric System. This policy also applies to JEA staff responsible for maintaining security and compliance with all activities pursuant to this cyber security policy or is responsible for such employees, agents, contractors and service vendors.

1.2 Definitions

Reference - NERC CAN 0010).

Annual – Within the calendar year and no more than 15 months between activities.

Bulk Electric System (BES) – As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

BES Cyber Asset – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

CIP Cyber Assets – Also referred as "CIP Covered Assets" are combination of BES Cyber System or assets, and their associated Electronic Access Control Systems (EACM) and Physical Access Control Systems (PACS).

CIP Senior Manager – A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-014.

Control Center – One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets – Programmable electronic devices and communication networks including hardware, software, and data.

Development Cyber Asset (DCA) – Cyber Assets outside the ESP used to develop software changes and updates for CCA but are not themselves CCA.

Electronic Access Control or Monitoring Systems (EACM) – Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point – A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter (ESP) – The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Emergency – Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System. Emergency conditions for JEA may also include personnel safety and security conditions that are unplanned or need specialized attention (e.g. emergency services, police, fire rescue etc.), These conditions may also include other unplanned/unforeseen events that have potential to impact normal operations (System or personnel).

Physical Access Control Systems (PACS) – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Owner –

> **Cyber Asset Owner** – Business unit managers/delegate with the authority for acquiring, creating, and maintaining information and information systems within their assigned area of control.
>
> **Process Owner** – Business unit managers responsible for CCA, with the authority for acquiring, creating, maintaining data and control systems, and responsible for authorizing access to these assets within their assigned area of responsibility (3R4 Information Sensitivity).

1.3 CIP Exceptional Circumstances

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

NERC CIP revised standards allows for CIP Exceptional Circumstance conditions for the following requirements –

CIP-004,R2.2; Exception if needed will be allowed to requirement for completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, during CIP Exceptional Circumstances.

CIP-004, R4.1; Exception will be allowed when processing to authorize based on need, as determined by JEA, except for CIP Exceptional Circumstances. This includes electronic access and/or unescorted physical access into a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-006, R2.1; Exception will be allowed to requirement of continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, during CIP Exceptional Circumstances.

CIP-006,R2.2; Exceptions will be allowed to the requirement of manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, during CIP Exceptional Circumstances.

CIP-007, R4.3; JEA will where technically feasible retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.

CIP-010,R3.3; JEA. prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

It is the responsibility of JEA SME operating under CIP exceptional circumstance to document appropriately and maintain reference logs where convenient. Documentation can be completed after the exceptional circumstance has been handled. Similarly tickets to formally log such event shall be created and all available information shall be submitted. All CIP Exceptional Circumstance(s), will be submitted to CIP compliance for review of records at the earliest after the circumstance has been handled.

Appendix 2 – List all personnel by role who have authority to declare, CIP Exceptional Circumstance. It is the responsibility of these personnel to notify CIP Compliance department, after declaring CIP Exceptional Circumstance.

1.4 Emergency Situations

Emergency Situations that impact safety or reliability have been classified as CIP Exception Circumstance. During a declared reliability, health, safety (fire, flooding, adverse weather, law enforcement) or system emergency involving assets covered under this policy, it may become necessary to deviate from policies and procedures until an end to the emergency has been declared or such time that the provisions can be reinstated without health or safety risk. The declaration of such emergencies may be a Qualifying Event based on Standard Operating Procedures or by external entities such as health, safety or security officials. During the deviation period, compensating measures will be taken to minimize security risks to assets covered under this policy.

In the event of deviation from the requirements of this policy, the CIP Senior Manager or delegate must be notified as soon as practical. During the deviation period, records must be retained that document:

- Description of emergency situation
- The requirements being deviated

- The start and ending time for the deviation period
- The compensating actions taken to reduce security risk during the deviation period

Once the emergency situation has ended or the need for deviation from this policy has ended, actions must be taken to assure security has not been compromised during the deviation period and to return the impacted assets to a compliant state. All emergency situation documentation must be recorded as an exception to policy.

In the event of a catastrophic event, i.e. loss of an entire facility to fire, the recovery plans and emergency situations will be modified to the extent necessary to recover the impacted assets in a new or temporary facility. The recovery duration, roles, and responsibilities to return the impacted assets to normal operations will be unique to the specific incident.

1.5 Accessibility

This policy shall, with the exception of the appendices, be available via JEA's Intranet site under MD's and Procedures

1.6 Enforcement

. Any employees found to have violated this policy, may be subject to disciplinary action, up to and including termination of employment. Any service vendor or contractor found to have violated JEA's NERC CIP program will be subject to corrective action up to and including permanent removal from authorized CCA and/or access to JEA facilities.

1.7 Retention

JEA shall keep documentation required by Standard CIP-002 through CIP-011 from the time of completion of previous CIP audit unless otherwise differentiated within the Standards (i.e. retaining security logs for 90 days, cyber security events for three years, etc) or directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time. In any case where the above terms are in conflict with the retention period specified by the approved CIP standards, the period specified in NERC CIP standards will take the precedence.

1.8 Review and Approval

In accordance with CIP-003, requirement R3, this policy shall be reviewed and approved at least annually by the assigned CIP Senior Manager. The annual review of Appendix A shall be documented in the Policy Revision History. Reviews and updates to contributing procedures and plans as identified in Appendix A will be completed by those persons identified in Appendices C, D and E. Changes to Appendices B, will be reviewed and approved separately and documented in the Appendix Revision History.

2.0 BES Cyber System Identification

1. JEA shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3

   - Control Centers and backup Control Centers;
   - Transmission stations and substations;
   - Generation resources;
   - Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
   - Special Protection Systems that support the reliable operation of the Bulk Electric System; and
   - For Distribution Providers, Protection Systems specified in CIP-002, Applicability section 4.2.1.

JEA process shall identify –

Each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
Each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
Each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

BES Cyber Systems not included in Sections 1.1 or 1.2 above that are associated with any of the following assets and that meet the applicability qualifications in NERC CIP-002 Section 4 - Applicability, shall be identified as a Low BES Cyber System. FERC approved standards do not require JEA to maintain a list of all such BES Cyber Systems.

2. JEA shall review the identifications in requirement of BES Cyber System identification process and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified BES Cyber Systems.
3. JEA CIP Senior Manager or delegate shall approve the list of identified BES Cyber Systems at least once every 15 calendar months, even if it has no identified BES Cyber Systems.

Note: For the purpose of consistency, Impact Rating Criteria (CIP-002-5.1 - Attachment 1) can be referenced from the NERC website.

3.0 Low BES Cyber System Protection

Due to significantly higher number of Low impact BES Cyber System (LBCS); JEA shall not identify individual BES Cyber System for the purpose of compliance. It is the responsibility of the system owner to maintain inventory of asset in order to maintain a safe and secure operation at these LBCS

Following Cyber Security Controls shall be applied for these Cyber Assets/Systems.

1. **Cyber Security Awareness:** JEA shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

2. **Physical Security Controls**: JEA shall control physical access, based on need as determined by the JEA, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

3. **Electronic Access Controls:** JEA shall:

3.1. For all Low Impact BES Cyber System where external routable connectivity is allowed, JEA shall implement a Low Impact BES Cyber System Electronic Access Point (LEAP) to permit only necessary inbound and outbound bi-directional routable protocol access; JEA shall implement a process required to control permissions wherever external routable connectivity is allowed, and

3.2. JEA shall implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

4. **Cyber Security Incident Response**: JEA shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1. Identification, classification, and response to Cyber Security Incidents;

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

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

4.4. Incident handling for Cyber Security Incidents;

4.5. 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

4.6. 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.

4.0 Personnel and Training

1. **Security Awareness Program**: JEA, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented Security Awareness Program that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. JEA's Security Awareness Program shall be applied at least annually to all its Low Impact BES Cyber System to reinforce cyber security practices and include associated physical security practices.

2. **Cyber Security Training Program**: JEA, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes the following content;

   2.1. Cyber security policies;
   2.2. Physical access controls;
   2.3. Electronic access controls;
   2.4. The visitor control program;
   2.5. Handling of BES Cyber System Information and its storage;
   2.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
   2.7. Recovery plans for BES Cyber Systems;
   2.8. Response to Cyber Security Incidents; and
   2.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

JEA shall require completion of the training specified prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
JEA shall require completion of the training specified at least once every 15 calendar months.

3. **Personnel Risk Assessment (Background Screening) :** JEA, for its high impact and medium impact BES Cyber Systems and associated CIP Covered Cyber Assets, shall implement one or more documented personnel risk assessment (PRA) programs to attain and retain authorized electronic or authorized unescorted physical access to collectively include;

   3.1. Process to confirm identity.
   3.2. Process to perform a seven year criminal history records check as part of each PRA that includes:
      3.2.1. Current residence, regardless of duration; and
      3.2.2. Other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.
   3.3. For cases where it is not possible to perform a full seven year criminal history records check, JEA shall conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.

3.4. JEA Criteria and the process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to requirement 1 through 3 of this section.

3.5. JEA process shall require documenting the criteria to evaluate criminal history records checks for authorizing access to the CIP covered assets at its high impact and medium impact BES Assets.

JEA shall document the PRA process also referred as background screening and ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 1 to 3 prior to granting access and at least once within the last seven years.

4. **Access Management Program*:*** JEA, for its high impact and medium impact BES Cyber Systems and associated CIP Covered Cyber Assets, shall document and implement an Access Management Program that includes;

4.1. Process to authorize based on need, as determined by the JEA business units, except for CIP Exceptional Circumstances. Following access will be controlled using this process:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

4.2. JEA process shall verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records and for electronic access.

4.3. JEA process shall verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the JEA determines are necessary.

4.4. JEA process shall verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the JEA determines are necessary for performing assigned work functions.

5. **Access Revocation*:*** JEA, for its high impact and medium impact BES Cyber Systems and associated CIP Covered Cyber Assets, shall document and implement an Access Revocation Program that will include the following;

5.1. A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).

5.2. For reassignments or transfers, the program will require that JEA revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that JEA determines are not necessary by the end of the next calendar day following the date that JEA determines that the individual no longer requires retention of that access.

5.3. For termination actions, the program will require that JEA revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

5.4. For termination actions at High Impact BES Cyber System and their associated EACMs, JEA Program shall require that JEA revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.

5.5. For all termination actions at High Impact BES Cyber System and their associated EACMs, JEA Program shall require change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that JEA determines that the individual no longer requires retention of that access. JEA shall document within 10 calendar days following the end of the operating circumstances, if a need is determined that extenuating operating circumstances require a longer time period for change the password(s).

5.0 Electronic Security Perimeter(s) and Electronic Access Points

For all High and Medium impact BES assets, JEA shall document a process to ensure that all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
For all High and Medium impact BES assets, where External Connectivity is applicable, JEA shall ensure that all External Routable Connectivity must be through an identified Electronic Access Point (EAP).

All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

For all High and Medium impact BES assets, JEA process shall ensure that all Electronic Access Points (EAP) require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. All JEA Access Points that generate log, JEA must ensure that explicit deny statements is applied in order to ensure that all failed access attempts are monitored and logged.

For all identified Dial-up EAPs, where technically feasible, JEA will perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets. JEA approved policy prohibits usage of Dial-up devices limiting ability to create Dial-up EAP. Annual JEA conducts Cyber Vulnerability Assessments to identify Dial-up devices enabled for dial-up connections. JEA's new Cyber Assets commissioning policy has multiple controls to prevent establishing of Dial-up EAP.

For all High and Medium impact Control Centers JEA process shall ensure one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

1. **Remote Access**: For all High and Medium impact BES Cyber Systems allowing Interactive Remote Access, BES assets, JEA shall document a process to ensure the following;

   1.1. Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
   1.2. For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
   1.3. Require multi-factor authentication for all Interactive Remote Access sessions.

6.0 Physical Security of BES Cyber Systems

1. **Physical Security Plan** – For all High and Medium impact BES assets, JEA shall implement one or more documented physical security plan(s) that collectively include;

1.1. Define operational or procedural controls to restrict physical access.
1.2. Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.
1.3. Where technically feasible, for all High Impact BES Cyber Systems and associated EACMs and PACS, JEA shall utilize two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.
1.4. Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
1.5. Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the designated personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.
1.6. Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
1.7. Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.
1.8. Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
1.9. Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
1.10. For all BES Cyber Systems and Protected Cyber Assets, JEA Physical Security Plan shall ensure to restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, JEA shall document and implement one or more of the following:
1.10.1. encryption of data that transits such cabling and components; or
1.10.2. monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
1.10.3. an equally effective logical protection.

2. **Visitor Control Plan** – JEA shall implement one or more documented visitor control program(s) that include each of the applicable requirements;

1.4. Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
1.5. Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor, except

during CIP Exceptional Circumstances.

1.6. Retain visitor logs for at least ninety calendar days.

3. **Maintenance and Testing Plan** – JEA shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively ensures maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.

7.0 Systems Security Management

1. **Ports and Services**: For all High and Medium impact BES Cyber Assets, associated EACM and PACS, JEA shall implement one or more documented processes to ensure the following;

   1.1. Where technically feasible, JEA shall enable only logical network accessible ports that have been determined to be needed by JEA, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open shall be deemed needed.

   1.2. JEA shall protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

2. **Security Patch Management**: For all High and Medium impact BES Cyber Assets, associated EACM and PACS, JEA shall implement one or more documented processes to ensure the following;

   1.3. A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that JEA tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

   1.4. At least once every 35 calendar days, JEA shall evaluate security patches for applicability that have been released since the last evaluation from the identified source or sources.

   1.5. For applicable patches identified in Part ii, within 35 calendar days of the evaluation completion, JEA shall take one of the following actions:

      1.5.1. Apply the applicable patches; or

      1.5.2. Create a dated mitigation plan; or

      1.5.3. Revise an existing mitigation plan.

   1.6. JEA shall ensure that mitigation plans shall include JEA's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

   1.7. For each mitigation plan created or revised in Part iii, JEA shall implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part iii is approved by the CIP Senior Manager or delegate

3. **Malicious Code Prevention:** For all High and Medium impact BES Cyber Assets, associated EACM and PACS, JEA shall implement one or more documented processes to ensure the following;

   3.1. Deploy method(s) to deter, detect, or prevent malicious code.

   3.2. Mitigate the threat of detected malicious code.

   3.3. For those methods that use signatures or patterns, JEA shall have a process for the update of the signatures or patterns. JEA process shall address testing and installing the signatures or patterns.

4. **Security Event Monitoring**: For all High and Medium impact BES Cyber Assets, associated EACMs and PACS, JEA shall implement one or more documented processes to ensure the following;

   4.1. JEA shall log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

- Detected successful login attempts;
- Detected failed access attempts and failed login attempts;
- Detected malicious code.

4.2. JEA shall generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

- Detected malicious code
- Detected failure of event logging.

4.3. Where technically feasible, JEA shall retain applicable event logs for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.

4.4. JEA shall review a summarization or sampling of logged events as determined by JEA at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

5. **System Access Controls:** For all High and Medium impact BES Cyber Assets, associated EACMs, and PACS, JEA shall implement one or more documented processes to ensure the following;

1.1 JEA shall have a method(s) to enforce authentication of interactive user access, where technically feasible.

1.2 Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

1.3 Identify individuals who have authorized access to shared accounts.

1.4 Change known default passwords, per Cyber Asset capability.

1.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

1.5.1 Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and

1.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.

1.6 Where technically feasible, for password-only authentication for interactive user access, JEA shall either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

1.7 Where technically feasible, JEA shall either:

1.7.1 Limit the number of unsuccessful authentication attempts; and

1.7.2 Generate alerts after a threshold of unsuccessful authentication attempts.

8.0 Incident Reporting and Response Planning

1. **Incident Response Plan** – JEA shall document a Cyber Security Incident response plan(s) that collectively include each of the applicable requirements;

    1.1 One or more processes to identify, classify, and respond to Cyber Security Incidents
    1.2 One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (E-ISAC), unless prohibited by law. Initial notification to the E-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.
    1.3 The roles and responsibilities of Cyber Security Incident response groups or individuals.
    1.4 Incident handling procedures for Cyber Security Incidents.

2. **Implementation and Testing** – JEA Cyber Security Incident response plan shall include the following requirements;

    2.1 Test each Cyber Security Incident response plan(s) at least once every 15 calendar month
    2.1.1 By responding to an actual Reportable Cyber Security Incident;
    2.1.2 With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or
    2.1.3 With an operational exercise of a Reportable Cyber Security Incident.
    2.2 Use the JEA Cyber Security Incident response plan(s when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.
    2.3 Retain records related to Reportable Cyber Security Incidents.

3. **Review, Update, and Communication** – JEA Cyber Security Incident response plan shall include the following requirements;

    3.1 Testing – No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:
    3.1.1 Document any lessons learned or document the absence of any lessons learned;
    3.1.2 Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and
    3.1.3 Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.
    3.2 Changes –No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan;
    3.2.1 Update the Cyber Security Incident response plan(s); and
    3.2.2 Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.

9.0 Recovery Plans for BES Cyber Systems

1. **Recovery Plans** – JEA for all its BES Cyber System, associated EACMs, and PACS shall document and implement recovery plans to collectively include each of the applicable requirements;

   1.1 Describe conditions for activation of the recovery plan(s).
   1.2 Document roles and responsibilities of responders.
   1.3 Document one or more processes for the backup and storage of information required to recover BES Cyber System functionality.
   1.4 Document one or more processes to verify the successful completion of the backup processes and to address any backup failures.
   1.5 Document one or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Documented procedure must consider that data preservation should not impede or restrict recovery.

2. **Implementation and Testing** – JEA Recovery plan shall be documented to ensure the following;

   2.1 All the recovery plans are tested at least once every 15 calendar months using any of the following methods:
      2.1.1By recovering from an actual incident;
      2.1.2With a paper drill or tabletop exercise; or
      2.1.3With an operational exercise.
   2.2 Once every 15 calendar months JEA shall test a representative sample of information used to recover BES Cyber System functionality to ensure that the information is useable and is compatible with current configurations or by completing an actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.
   2.3 JEA shall test each of the recovery plans at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment or by completing a successful actual recovery response instead of an operational exercise.

3. **Review, Update and Communication** – JEA shall document and ensure the following;

   3.1 No later than 90 calendar days after completion of a recovery plan test or actual recovery:
   3.2 JEA shall document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;
   3.3 Update the recovery plan based on any documented lessons learned associated with the plan; and
   3.4 Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.
   3.5 No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the JEA determines would impact the ability to execute the recovery plan:
   3.6 JEA shall Update the recovery plan; and
   3.7 Notify each person or group with a defined role in the recovery plan of the updates.

10.0 Configuration Change Management and Vulnerability Assessments

JEA shall implement one or more documented process(es) that collectively include each of the following requirements;

1. For all JEA High and Medium Impact BES Cyber Systems and their associated EACMS; PACS; and PCA, JEA shall develop a baseline configuration, individually or by group, which shall include the following items;

1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
1.2. Any commercially available or open-source application software (including version) intentionally installed;
1.3. Any custom software installed;
1.4. Any logical network accessible ports; and
1.5. Any security patches applied.

2. For all JEA High and Medium Impact BES Cyber Systems and their associated EACMS; PACS; and PCA;

2.1. JEA shall authorize and document changes that deviate from the existing baseline configuration.
2.2. For a change that deviates from the existing baseline configuration, JEA shall update the baseline configuration as necessary within 30 calendar days of completing the change.
2.3. For a change that deviates from the existing baseline configuration:
2.4. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
2.5. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
2.6. Document the results of the verification.

3. For all JEA High Impact BES Cyber Systems, where technically feasible, for each change that deviates from the existing baseline configuration;

3.1. Prior to implementing any change in the production environment, JEA shall test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
3.2. JEA shall document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

4. For all JEA High Impact BES Cyber Systems and their associated EACMS; and PCA, JEA shall implement one or more documented process(es) that monitor at least once every 35 calendar days for changes to the baseline configuration and document and investigate detected unauthorized changes.

5. For all JEA High and Medium Impact BES Cyber Systems and their associated EACMS; PACS; and PCA, include a Cyber Vulnerability Assessments program that will include –

5.1. At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

6. For all JEA High Impact BES Cyber Systems, where technically feasible, at least once every 36 calendar months:

6.1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and

6.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

7. For all JEA High and Medium Impact BES Cyber Systems and their associated EACMS; PACS; and PCA, prior to adding a new applicable Cyber Asset to a production environment, JEA shall perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

7.1. JEA shall document the results of the assessments conducted and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

JEA, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the following;

8. **Transient Cyber Assets and Removable Media:** Transient Cyber Asset(s) Managed by JEA shall implement a Transient Cyber Assets and Removable Media security program to address the following;

8.1. **Transient Cyber Asset Management**: JEA shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

8.2. **Transient Cyber Asset Authorization**: For each individual or group of Transient Cyber Asset(s), JEA program shall authorize:

8.2.1. Users, either individually or by group or role;

8.2.2. Locations, either individually or by group; and

8.2.3. Uses, which shall be limited to what is necessary to perform business functions.

8.3. **Software Vulnerability Mitigation**: For all Transient Cyber Assets, JEA shall use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;

- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

8.4. **Introduction of Malicious Code Mitigation**: For all Transient Cyber Assets, JEA shall use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (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.

8.5. **Unauthorized Use Mitigation**: For all Transient Cyber Assets, JEA shall use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

9. Transient Cyber Asset(s) Managed by a Party other than JEA.

9.1. **Software Vulnerabilities Mitigation**: For all Transient Cyber Assets, managed by a part other than JEA, JEA shall ensure use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

9.2. **Introduction of malicious code mitigation**: For all Transient Cyber Assets, managed by a part other than JEA, JEA shall ensure use one or a combination of the following methods to achieve the objective of mitigating malicious code (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 malicious code.

For any method used to mitigate software vulnerabilities or malicious code as specified in 9.1 and 9.2, JEA shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

10. Removable Media

10.1. **Removable Media Authorization**: For each individual or group of Removable Media, JEA program shall authorize:

10.1.1. Users, either individually or by group or role; and

10.1.2. Locations, either individually or by group.

10.2. **Malicious Code Mitigation**: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, JEA program shall:

10.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

10.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

11.0 Cyber Asset Information Protection

1. JEA shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011*, *R1 – Information Protection*. For JEA's high and medium impact BES Cyber Systems and their associated EACMs and PACS, JEA information protection program shall include the following;

1.1. A method(s) to identify information that meets the definition of BES Cyber System Information.

1.2. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

2. JEA shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011, R2 – BES Cyber Asset Reuse and Disposal. For JEA's high and medium impact BES Cyber Systems and their associated EACMs, PACS, PCAs, JEA information protection program shall address the following;

2.1. Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified above), JEA shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

2.2. Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, JEA shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

12.0 Appendix A: CIP Senior Manager Assignment

ASSIGNMENT OF RESPONSIBILITY:

The General Manager/Vice President (VP/GM) Electric Systems is assigned and authorized by the Managing Director/Chief Executive Officer to serve as the single Senior Manager with overall responsibility for CIP compliance and to assign specific delegation of authority as allowed by NERC CIP Standards and listed in Appendix B. The CIP Senior Manager is tasked with establishing the policies, procedures and plans to meet NERC CIP compliance. Designation of authorized approvers in accordance with CIP-004 shall be documented in Appendix C. Processes and Ownership for functional responsibilities under the CIP requirements shall be documented in Appendix D.

JEA CIP Senior Manager

Mike J. Brost

VP/GM Electric Systems

JEA, (16th Floor, JEA Tower)

21 West Church Street, Jacksonville, FL- 32202

ASSIGNED BY:

SIGNATURE: ______________________________
Managing Director/Chief Executive Officer

Date: ___________________

13.0 Appendix B: CIP Senior Manager Delegated Authority List

Functional Area	Delegated Actions Include	Name / Roles	Title	Phone	Date of Designation
BES Cyber System/Asset Identification	Review, document and approve the CIP-002 application of BES asset impact criteria	Garry Baker - Approver	Director, Electric Systems Operations	665-7145	3/1/2016
BES Cyber System/Asset Identification	Identify, document and approve CIP BES Cyber Assets and CIP Cyber Assets (CCA).	Daniel Mishra - Approver	Director, CIP Compliance	665-7655	3/1/2016
Physical Security	All aspects of physical security.	Patrick C. Maginnis - Approver	Director, Security	665-6070	3/1/2016
Mitigation Plan Extension	Extend time line for approved mitigation plan for applicable patches.	Daniel Mishra	Director, CIP Compliance	665-7655	3/1/2016
Exceptional Circumstance	Declaration of CIP Emergency condition/exceptional circumstance.(Operation)	Roles of BPO Shift Operators, Supervisors, Managers and Directors.	As Applicable	As Applicable	3/1/2016
Exceptional Circumstance	Declaration of CIP Emergency condition/exceptional circumstance.(System Protection)	Roles of Relay Foreman and Relay Tech, Supervisors, Managers and Directors.	As Applicable	As applicable	3/1/2016
Exceptional Circumstance	Declaration of CIP Emergency condition/exceptional circumstance (Security).	Managers, Directors (Physical Security) and Security Operation Shift Supervisor	As Applicable	As Applicable	3/1/2016
Exceptional Circumstance	Declaration of CIP Emergency condition/exceptional circumstance (Information Security)	Managers and Directors (Information Security and Technology Infrastructure)	As Applicable	As Applicable	3/1/2016
Exceptional Circumstance	Declaration of CIP Emergency condition/exceptional circumstance (Technology Infrastructure)	Network Operations Control - Shift Supervisor	As Applicable	As Applicable	3/1/2016

- Only personnel who have authorized unescorted access to PSP can declare CIP exceptional circumstance.

14.0 Appendix C: Relation Critical Infrastructure Responsibility Matrix

CIP	Functional Area	Procedure	Location
CIP-002 BES Cyber System Categorization	CIP Compliance	BES Cyber System Identification	See Director, CIP Compliance/Director Electric Systems Operations
CIP-003 – Security Management Controls	CIP Compliance	MD-202 Cyber Security Policy	See Director, CIP Compliance
CIP-004 Personnel and Training	CIP Compliance	Security Awareness program	Available on Quest*
	Human Resources	Personnel Risk Assessments	Available on Quest*
	Information Security	Access Administration	Available on Quest*
	CIP Compliance	CIP Cyber Security Training	See Director, CIP Compliance
CIP-005 Electronic Security Perimeter(s)	Technology Infrastructure	Electronic Security Perimeters	See Director, Technology Infrastructure
	Substation		See Director, Substation Projects
	Information Security	ESP Monitoring	See Director, Information Security
CIP-006 Physical Security of BES Cyber Systems	Physical Security	BES Cyber Systems Physical Security Plan	See Director, Physical Security
CIP-007 System Security Management	Technology Infrastructure	Security Patch Management & Ports and Services	Available on Quest*
	Information Security	Security Event Monitoring, System Access Controls & Malicious Code Prevention	See Director, Information Security
	Substation	System Change Control & System Security Process	See Director, CIP Compliance
CIP-008 Incident Reporting and Response Planning	Information Security	Cyber Incident Response	See Director, Information Security
	Physical Security	Physical Incident Response	See Director, Physical Security
	Substation	Substation Incident Response	See Director, Electric Trans. Mission & Substation Maint.
CIP-009 Recovery Plans for BES Cyber Systems	Technology Infrastructure	Recovery Plans for BES Cyber System/Assets/EACM/PACS	See Director, Technology Infrastructure
	Information Security		See Director, Information Security
	Substation		See Director, CIP Compliance
	Physical Security		See Director, Physical Security
	BPO		Director, Electric Systems Operations
CIP-010 Configuration Change Management & Vulnerability Assessments	Technology Infrastructure	Baseline, Configuration Change Management & Testing	Available on Quest*
	Information Security	Vulnerability Assessment	See Director, Information Security
	BPO		Director, Electric Systems Operations
	Substation	System Change Control & System Security Process	See Director, CIP Compliance
		CIP Security Controls & Configuration	See Director, CIP Compliance
CIP-011 Information Protection	Information Security	Information Protection Program	See Director, Information Security
	Technology Infrastructure	Cyber Asset Disposal & Redeployment	See Director, Technology Infrastructure

*User who do not have access to the Quest intranet website (such as remote contractors), should contact their JEA sponsor/coordinator or one of the following departments-

1. Department of Information Security
2. Department of CIP Compliance

15.0 Appendix D: Designated Access Authorization Authority

Functional Area	Designated Actions Include	Name	Title	Phone
Bulk Power Operations	Approve physical access to SOCC and BUCC for CCA and quarterly attestation.	Baker, William G.	Director, Electric Systems Operations	665-7145
Technology Infrastructure	Approve physical access to CC-3 datacenter and quarterly attestation.	Fore, Lavonia L (Bea)	Senior Executive	665-7217
EMS System	Approve logical and physical access to EMS CCAI and cyber access to EMS System.	Mayer, Andrew C	Manager, Bulk Power Operations	665-7111
Information Security	Approve cyber access to all tools used for cyber security, logical and physical access to CCAI pertaining to cyber security systems and quarterly attestation.	Kearson, William A	Director, Information Security	665-4306
Physical Security	Approve cyber access to AMAG administration and logical and physical access to physical security CCAI.	Patrick C. Maginnis	Director, Security	665-6070
Computer Operations, Help Desk and PC Support	Approval of cyber access for administration of EMS PCs, logical and physical access to PC CCAI and quarterly attestation.	Quarterman, Diane	Manager, Operations & Help Desk Support	665-4157
Technical Services	Approval of cyber access for Linux Server Administrators, logical and physical access to Linux server CCAI and quarterly attestation.	Datz, Stephen H.	Director, Technology Infrastructure	665-8872
Technical Services	Approval of cyber access for SAN Administrators, logical and physical access to SAN CCAI and quarterly attestation.	Datz, Stephen H	Director, Technology Infrastructure	665-8872
Technical Services	Approval of cyber access for server Administrators, logical and physical access to server CCAI and quarterly attestation.	Datz, Stephen H	Director, Technology Infrastructure	665-8872
Technical Services	Approval of cyber access for Oracle Database Administrators, logical and physical access to Oracle database CCAI and quarterly attestation.	Datz, Stephen H	Director, Technology Infrastructure	665-8872
Technical Services	Approval of cyber access for SQL Database Administrators, logical and physical access to SQL database CCAI and quarterly attestation.	Datz, Stephen H	Director, Technology Infrastructure	665-8872
Telecom & Wireless	Approval of cyber access for network Administrators, logical and physical access to network CCAI and quarterly attestation.	Traylor, Kymberly	Manager, Network & Telecommunications Services	665-8983
Substation Projects	All substation Compliance activities for new substation projects	Burbure, Vijay A	Director, Electric T&D Projects	665-6782
Substation Operations & Maintenance	All substation Compliance activities for Substation operation and maintenance.	Erixton, Ricky D	Director, Electric Transmission & Substation Maintenance	665-7110

SIGNATURE: ______________________

VP/GM Electric Systems

REVIEW/APPROVE DATE: 4-13-16

16.0 Policy & Appendix Revision History (for MD 202 Cyber Security Policy)

Revision #	Date	Description	Revised By	Approval
0	8/6/2007	Creation	RAP	WJK
1	8/4/2008	Annual review - no changes	RAP	WJK
2	7/30/2009	Annual Review - no changes	RAP	WJK
3	8/28/2009	Clarified procedures for emergency situations.	RAP	WJK
4	9/25/2009	Require full CIP Senior Manager signature in addition to initials	RAP	WJK
5	11/12/2009	Collated subset policies listed in Appendix A and incorporated delegation of authority list in Appendix B. Annual Review	RAP	WJK
6	10/1/2010	Annual Review. Collected compliance statements from various policies into single policy. Modify to reflect version 3 standards.	RAP	WJK
7	12/17/2010	Adjusted Appendix A to reflect CIP Compliance	RAP	WJK
8	1/7/2010	Annual Review. Modification of subordinate documents naming standard	RAP	WJK
9	10/1/2010	Annual Review.	RAP	WJK
10	3/16/2011	Annual Review. Modified CIP Senior Manager signature location	RAP	WJK
11	10/1/2011	Corrected Spelling Errors	RAP	WJK
12	6/13/2012	Annual Review	RAP	WJK
13	4/30/2013	Annual Review, CIP Review	DDM	WJK
14	3/21/2014	Annual Review, CIP Review	DDM	WJK
15	9/11/2014	Change in Senior Manager designation and delegation	DDM	MJB
16	5/11/2015	Annual Review, Responsibility Changes and updates	DDM	MJB
17	3/01/2015	MD-202Update for CIP V5 & V6	DDM	MJB

Note: CIP Senior Manager Signatures are required in two places, after the policy and after the appendices.