CORPORATE POLICY:	JEA Cyber Security Policy for Bulk Electric System (BES)		
VERSION EFFECTIVE DATE:	8/16/2024	**Version:**	26

POLICY STATEMENT:

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

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), SERC Reliability Corporation (SERC), 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, formerly referred to as MD-202, 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. This policy was formerly referred to as *MD-202 JEA Cyber Security Policy*. Upon approval of the current version, the title of this policy will be referred to as *JEA Cyber Security Policy for BES.* Any references in all of JEA's policies, procedures, and documentation, however previously mentioned or identified, shall hereby be deemed to refer to this policy.

ASSIGNMENT OF RESPONSIBILITY:

This policy applies to JEA employees, contractors, and vendors, with the business need for authorized logical 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 vendors.

Table of Contents

Definitions

Annual – Within the calendar year and no more than 15 months between activities. (Reference - NERC CAN 0010).
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 (BCA) – 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.
BES Cyber System Information (BCSI) –Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.
BES Cyber System Information (BCSI) Storage Location – A cyber asset or physical location which has been designated as a storage location in either physical or electronic format of BCSI. A Cyber Asset which has been designated as a BCSI Storage Location may additionally be classified as a Trusted Cyber Asset (TrCA) if the device has been classified as TrCA and has been designated to store BCSI.
CIP Cyber Assets (CCA) – 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 (CA) – Programmable electronic devices and communication networks including hardware, software, and data.
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.
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 (EAP) – 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).

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).

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.

Supplemental Workforce Staff Members – Personnel resources provided through all external agency contractors, as defined in JEA's Supplemental Workforce Staffing Policy. Such resources are generally managed under JEA Workspend contractors program.

Trusted Cyber Asset (TrCA) – Cyber Asset that is not already classified as BCA, EACMS, PACS, or PCA and

- Resides outside a designated CIP ESP and authorized to communicate using routable protocol to BCA, EACM, PACS, or PCA within ESP or;
- Whose operation is used for performing required function under NERC Reliability Standards.

A Cyber Asset which has been designated as a BCSI Storage Location may additionally be classified as a TrCA if the above conditions are met and the asset stores BCSI.

Vendor – Those persons, companies, or organizations with whom JEA or its affiliates contract with, to provide BES Cyber Systems or associated products and services. Does not include other NERC registered entities or personnel identified as Supplemental Workforce Staff Members.

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

CIP-003 Attachment 1 Section 5; Exception if needed will be allowed to requirement for 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.

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.

CIP-004, R6.1; Exception will be allowed when processing to authorize based on need, as determined by JEA, except for CIP Exceptional Circumstances. This includes provisioned electronic to electronic BCSI and physical access to physical BCSI.

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 will, 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.

CIP-010, R4; 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 sections in NERC CIP CIP-010, Attachment 1.

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 D – 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.

Emergency Situations

Emergency Situations that impact safety or reliability have been classified as CIP Exceptional 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.

Accessibility

This policy shall, with the exception of the appendices, be available upon request and via PolicyTech.

Enforcement

Any employees found to have violated this policy, may be subject to disciplinary action, up to and including termination of employment. Any 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.

Retention

JEA shall keep documentation required by all applicable NERC CIP Standards 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.

Review and Approval

In accordance with CIP-003, requirement R1, this policy shall be reviewed and approved at least annually by the assigned CIP Senior Manager. Appendix A identifies the assigned CIP Senior Manager. The annual review shall be documented in the Policy Revision History. Reviews and updates to contributing procedures, will be reviewed and approved separately and documented in the applicable procedures revision history.

Delegation of CIP Senior Manager Authority

In accordance with CIP-003, requirement R4, JEA 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. Appendix B includes all the Senior Manager delegations as applicable to JEA.

Roles, Responsibilities, and Segregation of Duties

Various departments of JEA are responsible for accomplishing the overall compliance objectives of this policy. Following section outlines the departmental level responsibilities and requires that departments must comply with the requirements of this policy and avoid any actions that conflict with the stated expectations or may result in non-compliance. Departmental heads are responsible and accountable for all actions taken by their department members affecting Compliance.

Subject Matter Experts: JEA personnel responsible for supporting, configuring, or administering JEA system must comply with compliance policy and procedures. If in any case, SME has concerns or confusion on compliance, all SME must communicate with their Departmental managers with copy to CIP Compliance department (CIPCompliance@jea.com)

Department Managers: Department Managers/Directors are responsible and accountable for all actions that affect compliance. For all concerns or clarifications related to compliance, Directors must communicate with CIP Compliance department (CIPCompliance@jea.com) in writing. Department must refrain from providing interpretation that conflict with the guidance provided by the CIP Compliance department. Any such conflict must be escalated to Chief Administrative Officer via appropriate Senior Leadership Member.

Director CIP Compliance: Director of CIP Compliance department is responsible for maintaining this policy, providing compliance guidance, communicating regulatory updates and changes to compliance requirements to all JEA departments. Director CIP is also responsible for all regulatory communications with enforcement agencies. Director CIP Compliance is responsible for providing any official interpretation for regulatory standard that is covered by this policy, and in case of any conflict, issues must be referred to the Chief Administrative Officer.

Senior Leadership: Senior Leadership Members (Chiefs/Vice-Presidents/General Managers) of JEA management team are responsible for leadership and oversight of this compliance program. Members of the team are also responsible for ensuring that various teams under their leadership comply with the compliance objectives set under this policy.

CIP Violations, Fact Findings, and Mitigation

In order to maintain compliance with NERC CIP standards, all JEA personnel responsible for CIP compliance shall ensure compliance with policy and procedures in place. However, if any non-compliance is detected/suspected, they must alert their Supervisor/Manager or CIP Compliance Department at the earliest opportunity, such that the violation impact can be limited. The process outlined in this section is applicable to all violations, regulatory violations as well as policy violations. Since this policy Cyber Security Policy for BES, addresses requirements broader than NERC CIP, some policy violations will only result in non-compliance with this policy.

1. In order to promote CIP compliance and build accountability to CIP compliance processes, all JEA Directors shall include an appropriate “Job Factors” for all JEA personnel involved with CIP Compliance.

2. If any violation is suspected or confirmed, it must be promptly (within one business day) reported to the CIP Compliance Department by emailing (cipcompliance@jea.com) or directly contacting JEA CIP Compliance personnel.
3. CIP Compliance will initiate a review of non-compliance incident and promptly (NLT 5 Business days) communicate with the department manager where non-compliance has been noticed.
4. Fact Finding - Department Manager/Supervisor, within seven (7) days from the date of notification/discovery, must initiate a Fact-Finding investigation (if bargaining unit) or Compliance Interview (if Appointed), to determine the following:
   4.1. Fact Finding or Appointed interviews must be initiated at the earliest opportunity so that facts are not lost and information is fresh.
   4.2. Fact Finding process must meet the JEA prescribed guidelines recommended for the bargaining units and include all factual details relevant to the incident as described by the participants.
   4.3. Following the completion of Fact Finding, all evidence must be compiled as confidential and a copy submitted to the CIP Compliance department as evidence.
   4.4. In consultation with CIP Compliance Department, determine that the violation is a confirmed violation of NERC CIP Requirement or a Cyber Security Policy violation
5. Root-Cause for the violation(s) - The root cause analysis must describe the factual details of the non-compliance, any contributing factors that lead to the non-compliance or should have prevented it, including the findings from the Fact Finding process.
   5.1. Vulnerability mitigation - Finalize step necessary and time required to correct the violation or any subsequent security vulnerability (Mitigation Action Plan), within 30 days from date of confirmation of the violation.
   5.2. The Department Manager/ Supervisor is responsible for completion of the corrective actions documented in the action plan (Mitigation Action Plan) and monthly reporting to CIP Compliance department on the progress of the approved Mitigation Action Plan.
   5.3. Measures required to control any reoccurrence of the violation including disciplinary actions if any.

Initiation of Root-Cause Analysis may be begin prior to, during, or post Fact Finding Investigation. A Root-Cause analysis is required to be completed and submitted to CIP Compliance, even if formal Fact Finding is not performed.

6. All mitigation action plans submitted by department Manager/Supervisor must be approved by CIP Compliance Department.
7. CIP Compliance department will be the custodian and maintain all the collected evidence. It will be responsible for conducting periodic review with CIP Oversight Committee. This committee will include Directors of JEA CIP stakeholder departments.

(This section intentionally left blank)

BES Cyber System Identification

JEA shall implement a process that considers each of the following assets -

- 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; one or more of the following facilities, systems, and equipment owned by the Distribution Provider for the protection or restoration of the BES:
  - Each UFLS or UVLS System that
    - Is part of load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
    - Performs automatic Load Shedding under a common control system owned by JEA, without human operator initiation, of 300MW or more.
  - Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Cranking Path and group of Elements meetings the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

JEA process shall identify –

- Each of the high impact BES Cyber Systems according to NERC Standard CIP-002 Attachment 1, Section 1, if any, at each asset;
- Each of the medium impact BES Cyber Systems according to NERC Standard CIP-002 Attachment 1, Section 2, if any, at each asset; and
- Each asset that contains a low impact BES Cyber System according to NERC Standard CIP-002 Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

BES Cyber Systems not included in High or Medium impact Rating that are associated with any of the following assets (listed above) 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.

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.
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.

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 implement electronic access controls to:
   3.1. Permit only necessary inbound and outbound electronic access as determined by JEA for any communications that are:
   3.1.1. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   3.1.2. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
   3.1.3. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
   3.2. Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability. Without express approval from CIP Compliance, dial-up connectivity shall not be allowed for any JEA BES CIP Cyber Assets.

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
   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.

5. **Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation**: JEA 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.

5.1. Transient Cyber Asset(s) Managed by JEA: JEA shall implement 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 updated of signatures or patterns;
- Application whitelisting
- Other method(s) to mitigation the introduction of malicious code.

5.2. Transient Cyber Asset(s) Managed by a party other than JEA: JEA shall implement the use of 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.

5.3. Removable Media: JEA shall implement the use of each of the following:

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

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

(This section intentionally left blank)

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 to as background screening and ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according 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; and
   4.1.2. Unescorted physical access into a Physical Security Perimeter;
   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 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.

5.4. 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).

6. **Access Management Program for BES Cyber System Information**: 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 for BES Cyber System Information that includes;

6.1. Prior to provisioning, authorized (unless authorized according to Part 4.1.) based on need, as determined by JEA, except for CIP Exceptional Circumstances:

6.1.1. Provisioned electronic access to electronic BCSI; and

6.1.2. Provisioned physical access to physical BCSI.

6.2. Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:

6.2.1. Have an authorization record; and

6.2.2. Still need the provisioned access to perform their current work functions, as determined by JEA.

6.3. For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to CIP-004 Requirement 5.1) by the end of the next calendar day following the effective date of the termination action.

(This section intentionally left blank)

Electronic Security Perimeter(s) and Electronic Access Points

1. **Electronic Security Perimeter**
For all High and Medium impact BES assets, JEA shall document a process to ensure that:
1.1. All applicable Cyber Assets connected to a network via a routable protocol reside within a defined ESP.
1.2. All External Routable Connectivity is through an identified Electronic Access Point (EAP).
1.3. All communication links between control centers shall be encrypted using secure tunneling technology or VPN in order to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers
1.4. 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.
1.5. 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.
1.6. 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.

2. **Remote Access**
For all High and Medium impact BES Cyber Systems allowing Interactive Remote Access, JEA shall document a process to ensure the following:
2.1. Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
2.2. For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
2.3. Require multi-factor authentication for all Interactive Remote Access sessions.
2.4. Have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
2.5. Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
2.6. All remote access activities to any CIP covered asset including BCA, PCA, EACM, and PACS shall be logged including authorized individual or resource, start and end of remote access, and comply with logging requirements of CIP-007, R4.

3. **Vendor Remote Access Management:** For all EACMS and PACS associated with High Impact BES Cyber Systems and all EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity, JEA shall document a process to ensure the following:
3.1. Have one or more method(s) to determine authenticated vendor-initiated remote connections.

3.2. Have one or more method(s) to terminate vendor-initiated remote connections and control the ability to reconnect.

(This section intentionally left blank)

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:
   2.1. 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.

2.2. 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.

2.3. 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.

(This section intentionally left blank)

Systems Security Management

1. **Ports and Services**: For all High and Medium impact BES Cyber Assets, Protected 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;
   2.1. 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.
   2.2. 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.
   2.3. For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, JEA shall take one of the following actions:
   2.3.1. Apply the applicable patches; or
   2.3.2. Create a dated mitigation plan (as per section 2.4); or
   2.3.3. Revise an existing mitigation plan.
   2.4. 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.
   2.4.1. SMEs shall, within 5 business days from the date of creation of a Mitigation Plan, notify CIP Compliance. CIP Compliance will review and approve all mitigation plans to ensure compliance with section 2.4.2 of this policy.
   2.4.1.1. All mitigation plans shall be part of Implementation change process, and must be created and approved before closing of the Implementation change.
   2.4.2. Mitigation Plan must satisfy the following criteria:
   2.4.2.1. Meet the intent and rigor of the CIP-007 Security Patch Management Requirement
   2.4.2.2. Provide a similar level of defense as the security patch itself, such that the mitigation plan sufficiently offsets the risk that the security patch was designed to defend against.
   2.4.2.3. Be above and beyond other CIP requirements. Existing CIP requirements cannot be considered as mitigation if they are already required for the applicable asset however, existing requirements may be combined with new security controls to become the mitigation plan.
   2.5. For each mitigation plan created or revised in Part 2.3, 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 2.3 is approved by the CIP Senior Manager or delegate.

3. **Malicious Code Prevention**: For all High and Medium impact BES Cyber Assets, PCA, 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;
   5.1. JEA shall have a method(s) to enforce authentication of interactive user access, where technically feasible.
   5.2. 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).
   5.3. Identify individuals who have authorized access to shared accounts.
   5.4. Change known default passwords, per Cyber Asset capability.
   5.5. For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:
      5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and
      5.5.2. 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.

5.6. 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.

5.7. Where technically feasible, JEA shall :

5.7.1. Limit the number to five unsuccessful authentication attempts; and

5.7.2. Generate alerts after a threshold of unsuccessful authentication attempts.

5.7.3. Account settings: In order to improve security, JEA CIP covered systems shall implement controls required by corporate security policy. For any conflicts between corporate requirements and CIP controls, higher security control shall be implemented.

5.8. If the system is technically capable of integration with Active Directory, then it must be integrated unless approved by the Senior Manager/Delegate or CIO.

5.8.1. If Systems allow a Hybrid model of AD integration, system access security shall be created only for system maintenance and support. All exceptions to this requirement shall be approved by the Manager IAM.

6. **Security Systems**: Due to increased security risks from emerging threats, for security systems (EACMs) associated to High BES Cyber Assets/Systems, where technically and operationally feasible, JEA shall implement the highest security measure allowed by the device configurations. Cases where such security measure is not feasible to implement due to operational or technical infeasibility, JEA SME shall document the justification during change control documentation.

Incident Reporting and Response Planning

1. **Cyber Security 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:

1.2.1 That include criteria to evaluate and define attempts to compromise;

1.2.2 To determine if an identified Cyber Security Incident is:

1.2.2.1 A Reportable Cyber Security Incident; or

1.2.2.2 An attempt to compromise, as determined by applying the criteria from 1.2.2.1, one or more systems covered under this policy; and

1.2.2.3 To provide notification to E-ISAC as required under this policy.

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 that attempted to compromise a system covered under this policy, 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 and Cyber Security Incidents that attempted to compromise a system covered under this policy.

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.
4. **Notifications and Reporting for Cyber Security Incidents –** JEA Cyber Security Incident Response Plan shall include the following requirements;
   - 4.1 Initial notifications and updates to E-ISAC, at a minimum, to the extent known:
     - 4.1.1 The functional impact;
     - 4.1.2 The attack vector used; and
     - 4.1.3 The level of intrusion that was achieved or attempted.
   - 4.2 Initial notifications made within the following timelines;
     - 4.2.1 One hour after the determination of a Reportable Cyber Security Incident.
     - 4.2.2 By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified covered under this policy.
   - 4.3 Update notifications, if any, within 7 calendar days of determination of new or changed attribute information.

(This section intentionally left blank)

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:
      2.1.1 By recovering from an actual incident;
      2.1.2 With a paper drill or tabletop exercise; or
      2.1.3 With 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.

Configuration Change Management and Vulnerability Assessments

1. **Configuration Change Management**: JEA shall implement one or more documented process(es) that collectively include each of the following requirements:

1.1. 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:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

1.1.3. Any custom software installed;

1.1.4. Any logical network accessible ports; and

1.1.5. Any security patches applied.

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

1.2.1. JEA shall authorize and document changes that deviate from the existing baseline configuration.

1.2.2. 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.

1.2.3. For a change that deviates from the existing baseline configuration:

1.2.3.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

1.2.3.2. Following the change, verify that required cyber security controls determined in 2.3.1 are not adversely affected; and

1.2.3.3. Document the results of the verification.

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

1.3.1. 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

1.3.2. 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.

1.4. For all JEA High & Medium Impact BES Cyber Systems and their associated EACMS and PACS:

1.4.1. Prior to a change that deviates from the existing baseline configuration associated with Paragraph 1 **Baseline Configuration,** Sub-paragraphs 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to JEA from the software source:

1.4.1.1. JEA shall verify the identity of the software source; and

1.4.1.2. JEA shall verify the integrity of the software obtained from the software source.

2. **Configuration Monitoring**: 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.

2.1. Audit account logon events – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit each instance of a user logging on to or logging off from another device in which this device is used to validate the account.

2.2. Audit account management – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit each event of account management on a device.

2.3. Audit directory service access – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.

2.4. Audit logon events – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit each instance of a user logging on to or logging off from a device.

2.5. Audit object access – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.

2.6. Audit policy change – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies.

2.7. Audit privilege use – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit each instance of a user exercising a user right.

2.8. Audit process tracking – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

2.9. Audit system events – JEA Information Security (JEA IS) determines and documents the configuration setting whether to audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.

2.10. All such setting will be defined and documented with CIP-008, Incident response objectives in sight and shall be documented in a manner that all SME involved with configuring system are able to meet the expectation of this policy and compliance assessment groups can verify if the SME have met the configuration requirements as per the policy.

3. **Cyber Vulnerability Assessments:** 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:

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

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

3.2.1. 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

3.2.2. 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.

3.3. 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.

3.4. 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.

(This section intentionally left blank)

Transient Cyber Assets and Removable Media:

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;

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

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.

   1.1. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), JEA program shall authorize:
   - Users, either individually or by group or role;
   - Locations, either individually or by group; and
   - Uses, which shall be limited to what is necessary to perform business functions.

   1.2. 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.

   1.3. 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.

   1.4. 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.

   1.5. Transient Cyber Asset(s) Managed by a Party other than JEA
   - 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.
- **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 above, JEA shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

2. Removable Media

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

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

2.1.2. Locations, either individually or by group.

2.2. 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:

2.2.1. 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

2.2.2. 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.

(This section intentionally left blank)

Cyber Security Information Protection

1. **Information Protection Program:** 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. Method(s) to identify BCSI.
   1.2. Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.

2. **BES Cyber Reuse and Disposal:** 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.

(This section intentionally left blank)

Cyber Security Control Between Centers

JEA shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. JEA plan shall include:

- JEA plan shall identify the security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- JEA plan shall identify where JEA applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- If the Control Centers are owned or operated by other Responsible Entities, JEA shall identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

(This section intentionally left blank)

Appendix A: CIP Senior Manager Assignment

ASSIGNMENT OF RESPONSIBILITY:
The Vice President/General Manager (VP/GM) Electric Systems is assigned and authorized by the President/Chief Operating 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-003 shall be documented in Appendix C.
List of all personnel by role who have the authority to declare, CIP Exceptional Circumstance shall be documented in Appendix D.

<u>**JEA CIP Senior Manager**</u>
Ricky Erixton
VP, Electric Systems
JEA, (7th Floor, HQ)
225 N. Pearl St., Jacksonville, FL 32202

ASSIGNED BY:

SIGNATURE: ___________________________________
Jay Stowe
- Managing Director, CEO

Date: ______________

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*	Identify, document, and approve BES Asset List and CIP BES Cyber Asset List.	Daniel Mishra – Approver	Director, CIP Compliance	665-7655	3/1/2016
Physical Security*	All aspects of physical security.	Brandon Edwards	Director, Security	665- 6584	3/1/2017
Mitigation Plan Extension*	Extend timeline for approved mitigation plan for applicable patches.	Daniel Mishra	Director, CIP Compliance	665-7655	3/1/2016
Supply Chain (CIP-013)*	Supply Chain Cyber Risk Management Plan review and approval.	Daniel Mishra	Director, CIP Compliance	665-7655	10/01/2020

- *CIP Senior Manager Delegations

Appendix C: Designated Access Authorization Authority

Functional Area	Designated Actions Include	Title
Bulk Power Operations	Approve physical access to SOCC and BUCC and quarterly attestation.	Sr Director Energy Operations
Technology Infrastructure	Approve physical access to CLGX datacenter and quarterly attestation.	Director, Network & Telecommunications Services
EMS System	Approve logical and physical access to EMS BCSI and cyber access to EMS System.	Manager, Bulk Power Operations
Information Security	Approve cyber access to all tools used for cyber security, logical and physical access to BCSI pertaining to cyber security systems and quarterly attestation.	Director, Information Security
Physical Security	Approve cyber access to AMAG administration and logical and physical access to physical security BCSI.	Director, Security & Emergency Preparedness
Computer Operations, Help Desk and PC Support	Approval of cyber access for administration of EMS PCs, logical and physical access to PC BCSI and quarterly attestation.	Manager, Service Desk Operations
Technical Services	Approval of cyber access for Linux Server Administrators, logical and physical access to Linux server BCSI and quarterly attestation.	VP, Technology Services
Technical Services	Approval of cyber access for SAN Administrators, logical and physical access to SAN BCSI and quarterly attestation.	VP, Technology Services
Technical Services	Approval of cyber access for server Administrators, logical and physical access to server BCSI and quarterly attestation.	VP, Technology Services
Technical Services	Approval of cyber access for SQL Database Administrators, logical and physical access to SQL database BCSI and quarterly attestation.	Manager, Technical Services
Telecom & Wireless	Approval of cyber access for network Administrators, logical and physical access to network BCSI and quarterly attestation.	Director, Network & Telecommunications Services
Substation Projects	All substation Compliance activities for new substation projects	Sr Director Engineering & Projects
Substation Operations & Maintenance	All substation Compliance activities for Substation operation and maintenance.	VP, Electric Systems

Appendix D: CIP Exceptional Circumstances

Functional Area	Delegated Actions Include	Name / Roles	Title	Phone	Date of Designation
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
Exceptional Circumstance	Declaration of CIP Emergency Condition/Exceptional Circumstance (Emergency Operations Center -EOC)	Any member of Active EOC or Extended EOC	As Applicable	As Applicable	6/8/2022

Only personnel who have authorized unescorted access to the PSP's can declare CIP exceptional circumstance.

Policy & Appendix Revision History

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	3/01/2016	MD-202Update for CIP V5 & V6	DDM	MJB
18	3/30/2017	MD-202 Update annual (minor corrections and updates)	DDM	MJB
19	11/07/2017	MD-202 Update – Added Roles and Responsibilities, addresses 2017 Mitigation Plan milestones	DDM	MJB
20	11/20/2018	MD-202 Update – Added section CIP Violations, Fact Findings an Mitigation (1.11)	DDM	MJB
21	1/15/2019	Update the delegation form for the Senior Manager. Separate the Senior Manager delegations (Appendix B) for the CIP Exceptional Circumstance (new Appendix E).	DDM	CBA
22	4/10/2020	Added new Security Requirements for Low BES Cyber Systems. Removed old appendix D reference to Standard/Procedure. Updated Job Titles throughout the document. Updated Accessibility for PolicyTech	KMD	CBA
23	5/03/2021	Annual update, CIP-012, Password policy update	DDM	RDE
24	6/29/2022	Revised title of document. Added updates for NERC Project 2019-03, includes updates to CIP-005-7 (Vendor Remote Access Management) and CIP-010-4 (EACMS and PACS). Updated Job Titles.	CDS/DDM	RDE
25	6/1/2023	Annual update, Replace CCAI with BCSI is multiple places, updated designations in Appendix C, updated language to address to CIP-004 and CIP-011 standard requirements	KMC	DDM
26	8/16/2024	Annual update, added TrCA and BCSI Storage Location definitions	KMC	

Policy Review & Approval

CIP Senior Manager Approval of Cyber Security Policy for BES and CIP Delegations

SIGNATURE: ___________-/Ricky Erixton, VP Electric Systems

REVIEW/APPROVE DATE: ___ __

APPROVED BY: Ricky Erixton, VP Electric Systems (Current Approver)

ORIGINAL EFFECTIVE DATE: 08/06/2007

Corresponding Procedures: *Contact appropriate personnel from Appendix C for corresponding procedures.