Policy Title:	Effective Date:	Last Modified Date:
Southern Company NERC Critical Infrastructure Protection Cyber Security Policy	December 1, 2012	November 29, 2012

Purpose

The purpose of this policy is to ensure the identification, security, and management of electronic and physical assets in a controlled manner and to comply with applicable company policies, industry practices, and Federal regulations. This policy is specifically intended to fully address the requirements of NERC CIP-002-3 through 009-3.

1. Policy Scope

For those assets covered by the NERC CIP-002-3 through 009-3 standards this policy supercedes all other cyber security policies.

This policy applies to all Southern Company and Affiliates' ("Company") employees, contractors, temporary and part-time workers, and those employed by others ("Users") to perform work on Company premises, or who have been granted access to Company information or electronic communication systems identified as Critical Cyber Assets according to the NERC CIP Cyber Security Standards.

This policy applies to electronic and physical assets for the purposes of compliance with NERC CIP-002-3 through 009-3.

2. Policy Statement

It is the policy of the Company to identify, secure, and manage electronic and physical assets in a controlled manner and to comply with applicable company policies, industry practices, and Federal regulations. Southern Company management fully supports this policy.

In case of emergencies designated by management, any deviations from this policy will be documented.

For the purposes of adherence to this policy, "annually" is defined as within a calendar year beginning January 1 and ending December 31. Events required annually by this policy should also occur no more than 15 months apart.

3. Policy Requirements

3.1 Standard CIP-002-3 – Cyber Security - Critical Cyber Asset Identification

R1. Critical Asset Identification Method. It is the policy of the Company to identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. It is the policy of the Company to maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

    a. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of the NERC CIP standards.

    b. Transmission substations that support the reliable operation of the Bulk Electric System.

    c. Generation resources that support the reliable operation of the Bulk Electric System.

    d. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

e. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

f. Special Protection Systems that support the reliable operation of the Bulk Electric System.

g. Any additional assets that support the reliable operation of the Bulk Electric System that the Company deems appropriate to include in its assessment.

R2. Critical Asset Identification. It is the policy of the Company to develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Company reviews this list at least annually, and updates it as necessary.

R3. Critical Cyber Asset Identification. It is the policy of the Company -- using the list of Critical Assets developed pursuant to Requirement R2 -- to develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. It is the policy of the Company to review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

2. The Cyber Asset uses a routable protocol within a control center; or,

3. The Cyber Asset is dial-up accessible.

R4. Annual Approval. It is the policy of the Company for the senior manager or delegate(s) to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on CIP-002-3 Requirements R1, R2, and R3, the Company may determine that it has no Critical Assets or Critical Cyber Assets. It is the policy of the Company to keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets, and the list of Critical Cyber Assets (even if such lists are null.)

3.2 Standard CIP-003-3 Cyber Security - Security Management Controls

R1. Cyber Security Policy. It is the policy of the Company to document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. It is the policy of the Company to, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2 The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership. It is the policy of the Company to assign a single senior manager with overall responsibility and authority for leading and managing its implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3 Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions. It is the policy of the Company that instances where the Company cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Company's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection. It is the policy of the Company to implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Company shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Company shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control. It is the policy of the Company to document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. It is the policy of the Company to maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1 Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2 It is the policy of the Company that the list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2 It is the policy of the Company to review at least annually the access privileges to protected information to confirm that the access privileges are correct and that they correspond with the Company's needs and appropriate roles and responsibilities.

R5.3 It is the policy of the Company to assess and document at least annually the process for controlling access privileges to protected information.

R6. Change Control and Configuration Management. It is the policy of the Company to establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

3.3   Standard CIP-004-3 Cyber Security – Personnel and Training

R1. Awareness. It is the policy of the Company to shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

1. Direct communications (e.g., emails, memos, computer based training, etc.);

2. Indirect communications (e.g., posters, intranet, brochures, etc.);

3. Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training. It is the policy of the Company to establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

a. The proper use of Critical Cyber Assets;

b. Physical and electronic access controls to Critical Cyber Assets;

c. The proper handling of Critical Cyber Asset information; and,

d. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. It is the policy of the Company to maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment. It is the policy of the company to have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Company shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Company may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Company shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Company shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.

R4. Access. It is the policy of the Company to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Company shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. It is the policy of the Company to ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Company shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within 7 calendar days for personnel who no longer require such access to Critical Cyber Assets.

3.4   Standard CIP-005-3 Cyber Security – Electronic Security

R1. Electronic Security Perimeter. It is the policy of the Company to ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. It is the policy of the Company to identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Company shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Company shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls. It is the policy of the Company to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), it is the policy of the Company to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. It is the policy of the Company to implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, it is the policy of the Company to implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

a. The processes for access request and authorization.

b. The authentication methods.

c. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

d. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner. Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. It is the policy of the Company to maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access. It is the policy of the Company to implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, it is the policy of the Company to implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, it is the policy of the Company to review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment. It is the policy of the Company to perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance. It is the policy of the Company to review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. It is the policy of the Company to ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and to review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. It is the policy of the Company to update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. It is the policy of the Company to retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

3.5   Standard CIP-006-3 Cyber Security – Physical Security

R1. Physical Security Plan. It is the policy of the Company to document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, it is the policy of the Company to deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems. Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

R3. Protection of Electronic Access Control Systems. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls. It is the policy of the Company to document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. It is the policy of the Company to implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access. It is the policy of the Company to document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access. Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. It is the policy of the Company to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Company's selected access control and monitoring method.

- Video Recording: Electronic capture of video images of sufficient quality to determine identity.

- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention. It is the policy of the Company to retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

R8. Maintenance and Testing. It is the policy of the Company to implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Company in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

3.6 Standard CIP-007-3 Cyber Security – Systems Security Management

R1. Test Procedures. It is the policy of the Company to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches,

cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. It is the policy of the Company to create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. It is the policy of the Company to document that testing is performed in a manner that reflects the production environment.

R1.3. It is the policy of the Company to document test results.

R2. Ports and Services. It is the policy of the Company to establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. It is the policy of the Company to enable only those ports and services required for normal and emergency operations.

R2.2. It is the policy of the Company to disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, it is the policy of the Company to document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management. It is the policy of the Company, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. It is the policy of the Company to document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. It is the policy of the Company to document the implementation of security patches. In any case where the patch is not installed, it is the policy of the Company to document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention. It is the policy of the Company to use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. It is the policy of the Company to document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, it is the policy of the Company to document compensating measure(s) applied to mitigate risk exposure.

R4.2. It is the policy of the Company to document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management. It is the policy of the Company to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. It is the policy of the Company to ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. It is the policy of the Company to ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. It is the policy of the Company to establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. It is the policy of the Company to review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. It is the policy of the Company to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. It is the policy of the Company to identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, it is the policy of the Company to have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, it is the policy of the Company to require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring. It is the policy of the Company to ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. It is the policy of the Company to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. It is the policy of the Company to maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. It is the policy of the Company to retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. It is the policy of the Company to review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment. It is the policy of the Company to establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, it is the policy of the Company to destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, it is the policy of the Company, at a minimum, to erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. It is the policy of the Company to maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment. It is the policy of the Company to perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance. It is the policy of the Company to review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

3.7 Standard CIP-008-3 Cyber Security – Incident Reporting and Response Planning

R1. Cyber Security Incident Response Plan. It is the policy of the Company to develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Company must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation. It is the policy of the Company to keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

3.8   Standard CIP-009-3 Cyber Security – Recovery Plans for Critical Cyber Assets

R1. Recovery Plans. It is the policy of the Company to create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises. The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control. Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore. The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media. Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

4. Policy Enforcement and Consequences

Compliance with this policy is mandatory for all individuals defined in the scope of this policy. The Company reserves the right to monitor activity for purposes of compliance. Company management at all levels is accountable for ensuring this policy and its associated standards and procedures are communicated and complied with in their respective organizational units.

For any questions regarding applicability or interpretation of the policy, please contact your management or the Operations compliance office. If a breach to this policy has occurred, or if you believe a breach may have occured, contact your management or the Operations compliance office immediately.

Violations or breaches of this policy will result in corrective action, which may include, but is not limited to:
- Dismissal of contracted third-party representatives
- Cancellation of contracts or service-level agreements
- Loss of access or other privileges
- Termination of employment

The maximum penalty may be imposed on the first offense and without prior warning.

5. Policy Ownership and Maintenance

This policy is owned by the Southern Company Operations Compliance Officer, and maintained under the direction of the Ethics Compliance Council. Requests for changes to the policy can be submitted to the Operations Compliance office.

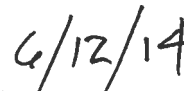This policy must be reviewed at least annually and more often if circumstances dictate.

6. References

Cyber Security Exception Form

7. Approved

Kim Greene
Executive Vice President & Chief Operating Officer
NERC CIP Senior Manager
Southern Company

6/12/14
Date Reviewed/Approved

Change Log:

Version	Date	Description	Author
0	06/03/2011	Initial Issue to consolidate policies and match the wording of the NERC CIP-002-3 through 009-3 standards.	Operations Compliance
1	06/04/2012	Review documents in preparation of NERC CIP Manager annual review. No content changes.	Operations Compliance
2	11/29/2012	Updates to section 3.2 in regards to CIP-003-3 R5 to aggregate NERC CIP information protection policy for NERC CIP Senior Manager review and approval.	Operations Compliance
3	06/11/2013	Review documents in preparation of NERC CIP Manager annual review. No content changes.	Jennifer Couch
4	05/16/2014	Review documents in preparation of NERC CIP Manager annual review. No content changes.	Jennifer Couch