AVANGRID

CORPORATE SECURITY / CYBERSECURITY

17 June 2019

Avangrid Data Classification and Treatment Rule

Document:	Data Classification and Treatment Rule
Date:	17 June 2019
Purpose:	Protection of Avangrid's information and data assets throughout lifecycle.
Owners:	Avangrid Corporate Security Office
Review & Update:	Periodically, the Owner shall review and update this document. The date of review and approval shall be noted in the table below.

Avangrid Corporate Security:



AVANGRID

17 / June / 2019

Avangrid Data Classification and Treatment Rule

Document:	Data Classification and Treatment Rule
Date:	17 June 2019
Purpose:	Protection of Avangrid's information and data assets throughout lifecycle.
Owners:	Avangrid Corporate Security Office
Review & Update:	Periodically, the Owner shall review and update this document. The date of review and approval shall be noted in the table below.

Avangrid Corporate Security:

June 20, 2019	Felicia Brown	Felicia Brown	VP CSO
Date	Name	Signature	Title

Avangrid Version History:

Version	Document	Author	Reason for Issue/Change	Date
V1.0	IUSA Information/Data Asset Classification Rule	J. Teller-Kanzler	Classification and treatment of information/data assets.	12/09/2014
V2.0	Avangrid Information/Data Asset Classification Rule	J. Teller-Kanzler	Updated to include additional clarifications.	06/02/2016
V3.0	Avangrid Information/Data Asset Classification Rule	J. Teller-Kanzler	Updated to align with industry and global best practices. Legal Review.	06/17/2019

--- CONFIDENTIAL ---
CORPORATE SECURITY / CYBERSECURITY
Take care of the environment. Printed in black and white and only if necessary. 1

Table of Contents

1. Purpose 3
2. Scope 3
3. Definitions 3
4. Rule Requirements and Controls 6
4.1. Information/data Asset Classification 6
4.2. Information/data Marking/Labeling 6
4.3. Data Protection Measures 7
5. Roles & Responsibilities 8
5.1. All Employees 8
5.2. Information Asset Owner 8
5.3. Information Asset Custodian 8
5.4. Managers and Business Area Leads (BALs) 8
5.5. Vendors and Contractors 9
5.6. Legal Services 9
5.7. Business/Corporate Functions 9
5.8. Corporate Security 9
5.9. Exceptions 10
Appendix A – Avangrid Data Classification Matrix 11
Classifying Avangrid Information/Data throughout its Life Cycle: 11

1. Purpose

Protection of Avangrid's cyber, physical and information assets is driven by business, legal, regulatory, financial and operational requirements.

The purpose of this *Avangrid Data Classification and Treatment Rule* (the "Rule") is to assist users in classifying business information/data assets and identifying the applicable security measures recommended to reduce the risk of unauthorized access, disclosure, alteration and destruction of Avangrid information/data assets. This Rule identifies a set of controls to be used to classify information/data assets based on their level of sensitivity, value and criticality to Avangrid.

This Rule shall be used in collaboration with the *Avangrid Cyber Asset Management Rule* and in conjunction with related policy and rules and appropriate processes, procedures and reviewed periodically to ensure that it remains current with Avangrid's legal, regulatory and compliance obligations.

This Rule and associated guidance was developed based on current industry best practice, guidance and standards.

2. Scope

This Rule applies to Avangrid, Inc. and all its subsidiaries (collectively "Avangrid").This Rule applies to information/data that is generated, accessed, modified, transmitted, stored or used, irrespective of the medium on which the information/data resides and regardless of its format (e.g. electronic, paper, audio, and video).

For purposes of this Rule, the words "information" or "data" can be used interchangeably.

3. Definitions

The purpose of the following definitions is to facilitate a common understanding of the relevant concepts included in this document.

- **Bulk Electric System** (BES) means transmission elements operated at 100 kV or higher and real power and reactive power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.
- **Bulk Power System** (BPS) means the facilities and control systems necessary for operating an interconnected network (and any portion thereof) and electric energy from generation facilities needed to maintain transmission system reliability. The term excludes facilities used in local electric distribution.
- **Business Area Lead (BAL)** is an internal Vice President or higher that is authorized to approve the sharing of confidential or restricted information.
- **Critical Energy/Electric Infrastructure** means a system or asset of the Bulk Power System, whether physical or virtual, the incapacity or destruction of which would negatively affect

national security, economic security, public health or safety, or any combination of such matters

- **Critical Energy/Electric Infrastructure Information (CEII)** means information related to critical electric infrastructure, or proposed critical electric infrastructure, generated by or provided to the Federal Energy Regulatory Commission (FERC) or another Federal agency other than classified national security information, that is designated as critical electric infrastructure information. CEII is (a) specific engineering, vulnerability, or detailed design information about a proposed or existing critical infrastructure that: (i) relates details about the production, generation, transportation, transmission, or distribution of energy, (ii) could be useful to a person in planning an attack on critical infrastructure, (iii) is exempt from mandatory disclosure under the Freedom of Information Act, and (iv) does not simply give the general location of the critical infrastructure.
- **Critical infrastructure:** means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.
- **Cyber-infrastructure:** includes electronic information and communications systems and services and the information contained in these systems and services. Those systems and services are composed of all hardware and software that process (creation, access, modification, and destruction), store (paper, magnetic, electronic, and all other media types), and communicate (sharing and distribution) information, or any combination of all of these elements.
- **Employee** is defined as all permanent staff, which is employed by Avangrid or on behalf of Avangrid. This includes on-assignment (temporary) fixed term staff.
- **Information/data Assets** are information and information systems that process, manage and organize the information in such a way that provides meaning or has value to business, such as customers systems/ databases, contracts and agreements, system documentation, research information, management systems, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information.
- **Information Custodian** is responsible for providing a secure infrastructure in support of the information/data asset, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to users as authorized by the Information Asset Owner.
- **Information Asset Owner** is a manager or above (or their designees) who are responsible for determining the sensitivity level of information/data asset(s) and classifying those assets according to their sensitivity and value to Avangrid. Information Asset Owners are also responsible for changing the classification level of these assets when warranted.
- **NERC Confidential** means: 1) information that by itself will not provide a high probability for a malicious actor to plan or cause a disturbance on the Bulk Electric System (BES), 2) information which may be obtained by any employee but should not be released to the public, and 3) information which may contribute to understanding or identifying an essential system. Information classified as NERC Confidential does not contain enough detail to be able to compromise assets, but may contribute to an attacker's knowledge of the essential system.

- **NERC Restricted** means information that by itself significantly increases the probability that a malicious actor can successfully compromise an essential system or plan, or execute an action that causes a disturbance on the Bulk Electric System (BES).
- **Personal Risk Assessment (PRA)** as defined in the North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard 004-1, ensures that a background check has been performed on those individuals electronically accessing or physically touching critical cyber assets.
- **User** is defined as any Employee, Contractor, Consultant or other Third Party with access to or use of Avangrid Electronic Devices or Cyber-infrastructure, regardless of their employment status.

4. Rule Requirements and Controls

4.1. Information/data Asset Classification

4.1.1. Information/data assets produced, owned or managed by Avangrid to provide services and achieve professional (business) objectives shall be *classified and prioritized,* throughout their lifecycle, based on the potential impact to the business in the event of a compromise or loss[1].

a. Classifying information/data assets shall be used to determine the appropriate protection measures required to reduce the risk of compromise or loss.

4.1.2. Classification levels shall be determined based on information/data asset type (e.g. Critical Electric/Energy Infrastructure Information - CEII, Personally Identifiable Information - PII) and criticality/value to Avangrid.

4.1.3. Information/data assets shall be assigned a classification level at inception and reviewed and adjusted as necessary throughout the assets' lifecycle.

4.1.4. Avangrid information/data assets shall be assigned one (1) of four (4) classification levels, as defined in the Avangrid Data Classification Matrix (Appendix A).

a. The four (4) categories that shall be used to classify Information/data assets produced, owned or managed by Avangrid are:

- **Public** – Information or data lawfully, properly and regularly disclosed generally or broadly to the public. Information that is neither sensitive nor controlled.
- **Internal Use** – Information or data that is needed to perform job responsibilities. Data is not approved for public disclosure; however, access is unrestricted within the company.
- **Confidential (including, without limitation, NERC Confidential)** – Information or data whose unauthorized disclosure, particularly outside Avangrid, could cause damage to our company, customers, employees or environments or be in violation of federal and/or state requirements.
- **Restricted (including, without limitation, NERC Restricted and CEII)** – Information or data considered secret and highly sensitive, whose unauthorized disclosure could result in grave damage, significant loss of customer or regulatory confidence, damage to Avangrid's reputation or put our employees at risk.

4.2. Information/data Marking/Labeling

4.2.1. Information/data assets produced, owned or managed by Avangrid to provide services and achieve professional (business) objectives shall be marked and/or labeled based on their classification; as per the Avangrid Data Classification Matrix (Appendix A).

[1] Compromise or loss such that the information/data becomes inaccessible, corrupted, destroyed, or made available to those who should not have access to it.

4.2.2. Where a set of information/data includes elements with varying assigned classification levels, the highest level in the set shall be used for marking/labeling.

a. The associated classification protections shall be applied to the set as a whole.

4.2.3. Specific marking and/or labeling shall be applied as follows:

a. Document: in the document footer (as per templates) on all pages, and in the metadata[2].

b. Emails: in the mail subject. In this case, the owner shall be the sender.

c. Multimedia files: In the metadata.

d. Removable media (e.g. CD, DVD, thumb drives, etc.) shall be marked with the highest level of classification based on the elements stored on the removable media and handled in accordance with the Data Classification Matrix.

e. Conversations: all parties shall be informed upfront if the information that is going to be discussed is Confidential or Restricted.

4.2.4 Unlabeled/unmarked Avangrid information/data assets shall be treated as information/data assets carrying the classification level of Internal Use.

4.3. Data Protection Measures

4.3.1. Controls to protect Avangrid information/data assets shall be applied throughout the assets' lifecycle, and shall be based on the assigned classification level.

a. Copies of Avangrid information/data assets shall be subject to the same protection controls as the original asset.

4.3.2. Information/data protection measures for electronic files shall also be applied and include:

a. Not storing Avangrid owned information/data on personal or non-Avangrid controlled or authorized environments.

b. Not sending Avangrid owned information/data through email to personal email accounts.

c. Using corporate storage spaces and network resources for file storage and/or exchange of Avangrid owned information/data.

i. Critical business information/data or information/data subject to legal or regulatory retention requirements shall not be stored on users' local hard drives.

d. Where an End Point Storage Device (EPSD) is required, only Avangrid supported and distributed devices, with the appropriate security measures shall be used.

e. Protection measures shall be adhered too for information/data assets as specified by regulations like Sarbanes-Oxley (SOX), NERC-CIP, the Payment Card Industry-Data Security Standard (PCI-DSS), etc.

[2] Metadata – includes data associated with either an information system or an information object for purposes of description, administration, legal requirements, technical functionality use and usage and preservation.

5. Roles & Responsibilities

5.1. All Employees

5.1.1 All employees shall handle Avangrid information/data assets in accordance with the classification level assigned.

5.1.2 All employees shall report the loss or misuse of marked/labeled information/data to their manager, the Information Asset Owner and Corporate Security at corporate.securityusa@avangrid.com.

5.1.3 Any employee who believes that an Avangrid information/data asset is improperly marked or labeled should immediately notify the Information Asset Owner.

5.2. Information Asset Owner

5.2.1 An Information Asset Owner shall be assigned to each information/data asset or group of information assets.

5.2.2 The Information Asset Owner shall determine the information/data assets' classification level and ensure the level accuracy throughout the assets' lifecycle.

5.2.3 The Information Asset Owner shall ensure that the information asset is clearly marked/labeled and that the marking/labeling remains accurate throughout the assets' lifecycle.

5.2.4 The Information Asset Owner shall ensure compliance with use and disclosure restrictions applicable to the information/data assets (e.g. as a result of confidentiality agreements with third parties, legal or regulatory requirements).

5.2.5 The Information Asset Owner shall ensure that the information/data asset is adequately deleted or destroyed at the end of its lifecycle.

5.3. Information Asset Custodian

5.3.1 An Information Asset Custodian shall be assigned to each information/data asset or group of information assets.

5.2.2 The Information Asset Custodian shall ensure that the technical security requirements are implemented to protect the asset, based on the assigned classification level and the Information Asset Owners' specific requirements.

5.4. Managers and Business Area Leads (BALs)

5.4.1 Managers and BALs shall be responsible for:

a. Promoting local implementation and compliance to this Rule.

b. Ensuring the integration of the Rule in Business processes and procedures.

c. Taking appropriate action when a breach or non-conformance with the rule is suspected or confirmed, including notifying Corporate Security.

d. Making the resources needed for compliance to the rule available.

e. Approving, for business reasons, exceptions to information/data sharing controls as required by this Rule.

f. Ensuring the submission of a security Third Party Risk evaluation for each new (or renewal) vendor/contractor engagement. (Determines the type and level of access to Avangrid owned information/data assets)

5.5. Vendors and Contractors

5.5.1 The security Third Party Risk management process shall be used to determine the type information/data asset and level of access required by a third party.

5.5.2 Execution of a non-disclosure agreement (NDA), confidentiality agreement or other agreement that includes appropriate non-disclosure and confidentiality provisions approved by the Avangrid's Legal Services shall be required before granting access to Avangrid Information/data assets classified as Confidential or Restricted.

5.5.3 Vendors/contractors requiring access to Avangrid information/data assets shall be required to complete a Third Party Risk Assessment.

5.5.4 Results of the assessment shall demonstrate established process and controls to protect Avangrid information/data assets.

5.5.5 Contractors requiring access to information/data assets subject to NERC-CIP Standards shall be required to complete NERC-CIP training.

5.5.6 Contractors requiring access to information/data assets subject to NERC-CIP Standards shall be required to have a Personal Risk Assessment (PRA) Check performed.

5.6. Legal Services

5.6.1 As needed and in accordance with Avangrid Records and Information Management Rule, shall provide legal advice to the Business/Corporate Areas in the identification of retention periods derived from legal or regulatory requirements or related to the need to address potential claims.

5.7. Business/Corporate Functions

5.7.1 Business Areas/Corporate Functions shall be responsible for:

a. Identifying the required technical tools and technologies needed to meet the defined controls.

b. Provisioning and implementing the necessary organization and technical controls (as defined) to support the Rule.

c. Defining the retention schedules in accordance with Avangrid Records and Information Management Rule.

d. Technical security monitoring and measurement to ensure that technical controls are working as expected.

d. Ensuring compliance to the Rule.

5.8. Corporate Security

5.8.1 Corporate Security shall be responsible for:

a. Governance, oversight and maintenance of the rule.

b. Providing guidance, recommendations, and clarifications to users in regards to the Rules' content.

c. Providing training and awareness related to the Rule.

5.9. Exceptions

Any relevant exception to this Rule that could entail a significant risk to Avangrid shall be approved using the Avangrid Exception Management Procedure. As required by procedure, any request for exception must be made in writing accompanied by supporting business documentation justifying the exception.

Appendix A – Avangrid Data Classification Matrix

The Avangrid Data Classification Matrix can be found in its entirety at: http://iusaintranet/mycompany/iberdrolausa/security/Cyber%20Security%20Policies/Forms/AllItems.aspx

Classifying Avangrid Information/Data throughout its Life Cycle:

1. Prior to information/data creation consider information/data classification requirements:

AVANGRID Data Classification Matrix				
Type	**Non-Sensitive**		**Sensitive**	
Avangrid Data Classification	**Public**	**Internal Use**	**Confidential NERC Confidential**	**Restricted - Secret NERC Restricted CEII**
Global Data Classification	**Public**	**Internal Use**	**Confidential**	**Restricted-Secret**
Risk	Low Risk	Medium risk	High risk	Very high risk
Description	Information or data lawfully, properly and regularly disclosed generally or broadly to the public. Routine office correspondence available to the general public. Typically regarded as information in the public domain.	Information or data employees have access to that is needed to perform their job responsibilities. Information or data is not approved for public disclosure. Information or data that is valuable to AVANGRID, unauthorized disclosure/destruction could cause damage to AVANGRID.	Information or data whose unauthorized disclosure, particularly outside AVANGRID, would cause damage to AVANGRID, loss of customers, embarrassment to the company, or would be in violation of federal and/or state regulatory requirements resulting in fines or litigation against AVANGRID.	Highly sensitive or valuable information or data, whose exposure, unauthorized disclosure/destruction would result in grave damage, significant loss of customer confidence, loss of market share and damage to AVANGRID's reputation. Could put staff and/or customers at risk.
Criteria	Information or data which can be made available to anyone without exception. It is neither sensitive or nor controlled.	Information or data which AVANGRID management believes requires limitations on internal access on a "need-to-know" basis, but which does not fall under the definition of 'sensitive information'. Not covered under any federal or state legislation.	Information or data which must be available in order for AVANGRID to effectively perform its mission and meet legally, assigned responsibilities. If lost or damaged could cause significant financial loss, inconvience or delay in performance of services and result in loss of public trust. May create risk for the Bulk Electric System, Bulk Power System, critical energy/electric infrastructure, or critical infrastructure.	Information or data that has limitations placed upon its internal access and that may be disclosed only in accordance with public law, federal statute, and supporting AVANGRID policies, rules, guidelines, procedures and processes. Would create risk for the Bulk Electric System, Bulk Power System, critical energy/electric infrastructure, or critical infrastructure.
Information/Data Examples	Marketing Materials authorized for public release such as advertisements, brochures, web pages, catalogues, external hiring notices, information found in the AVANGRID Annual Report.	Business plans, marketing strategies, internal memos, directives, training materials, organizational charts, generic maps/diagrams. Authorized access lists for BES Cyber Systems, training materials.	Information or data that falls under privacy related statutes, nonpublic personal customer, consumer or employee information, incident response plans, operating plans, operating procedures, transaction data, productivity reports, disciplinary reports, contracts, Service level Agreements, floor plans of NERC computing centers that show BES Cyber Systems, network topology or similar diagrams for NERC CIP ESP related networks, etc.	Business strategies, product development, merger and acquisition information, notes restricted to senior executives and most accounting data. Passwords, passphrases, password databases, and PIN codes, VPN tokens, credit and debit card numbers. Personally identifiable information (e.g. PII, social security numbers). Security configuration (e.g. BES Cyber Systems, and ESP or PSP equipment). IP addresses, hostnames in context of CIP assets where it can be used to obtain IP addresses, ESP Firewall Rules, etc.

2. Information/data Creation:

Life-Cycle: Creating				
Marking/Labeling Documents (paper and electronic, including web pages)	No special requirements	Mark each page on hard copy as 'Internal Use'. Identify electronic information as 'Internal Use'.	Mark each page on hard copy as 'Confidential' or 'NERC Confidential'. Identify electronic information as 'Confidential' or 'NERC Confidential'. Include a legend stating restrictions.	Mark each page on hard copy as 'Restricted' or 'NERC Restricted'. Identify electronic information as 'Restricted' or 'NERC Restricted'. Include delivery instructions.
Reproduction	Unlimited	Unlimited copies may be made by AVANGRID employees. Must include 'Internal Use' marking.	Limited copies may be made internally or externally with approval (permission) by information and/or data owner; consistent with the need to carry out job responsabilities. If digital copies are used, cache must be erased.	Limited copies may be made internally or externally with approval (permission) by information and/or data owner; consistent with the need to carry out job responsabilities. Proof of approval (permission) must be available upon request. If digital copies are used, cache must be erased.

3. Information/data Transmission (Distribution)

Life-Cycle: Transmission (Distribution) of information or data				
Internal mail within AVANGRID	No special requirements	Internal routing envelope/container with no special markings.	Sealed internal mail envelope, marked and labeled.	Routing envelope sealed, hand delivered where feasible.
Extended AVANGRID subsidiaries & other offices	No special requirements	Sealed envelope/container marked 'Internal Use'.	Sealed envelope/container marked 'Confidential' or 'NERC Confidential', To opened by addressee only'.	Sealed envelope/container marked 'Restricted' and restricted to a specified individual. Trackable delivery required.
Facsimile within AVANGRID	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public.	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public.	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public. Requires notification and verification of receipt. Sender and receiver must be at fax machines until transmission is complete.	Should not be used. If need to use, Requires Fax cover sheet. Fax machine should be located in a secured area. Telephone notification prior to transmission and subsequent telephone confirmation of receipt required. Immediately confirm receipt. Sender and receiver must be at fax machines until transmission is complete.
Facsimile overseas	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public.	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public.	Requires Fax cover sheet. Fax machine should be located in an area not assessable to the general public and unauthorized employees. Requires notification and verification of receipt. Sender and receiver must be at fax machines until transmission is complete.	Must not be used.
Email within AVANGRID	No special requirements	None	Encryption required for transmission.	Use of email discouraged unless encrypted.
Email outside AVANGRID	No special requirements	Encryption required for transmission to external email addresses	Encryption required for transmission to external email addresses.	Use of email discouraged.
Transmission by Spoken Word	No special requirements	Reasonable precautions to prevent inadvertent disclosure.	Active measures and close control to limit information to as few persons as possible.	Active measures and close control to limit information to as few persons as possible.

4. Information/data Storage

Life-Cycle: Storage				
Hardcopy Storage within AVANGRID	No special requirements	Can leave in closed desk or unattended cabinet. Reasonable precautions to prevent access by non-employees.	Requires reasonable care. Storage in lockable enclosure, e.g. desk or storage cabinet.	Requires extreme care. Locked in desk, safe or storage cabinet when unattended. Access should be highly restricted.
Hardcopy Storage off site	No special requirements	Information must be in control of individual entrusted with the information.	Information must be in control of individual entrusted with the information.	Information must be in control of individual entrusted with the information.
Electronic documents	Stored on owner's drive	Stored on owner's drive	Storage on secure drives only. Password protection of document preferred.	Storage on secure drives only. Password protection/encryption of document required.
E-mail	No special requirements	Reasonable precautions to prevent access by unauthorized personnel.	Encrypted storage and backup in a secure location or container.	Encrypted storage and backup in a secure location or container.

5. Information/data Destruction and Disposal

Life-Cycle: Destruction & Disposal				
Hardcopy within AVANGRID	Regular Trash, recycle	Follow department record retention guidelines for shredding (cross cut) or secure shreding receptables.	Follow department record retention guidelines for shredding (cross cut) or secure shreding receptables.	Follow department record retention guidelines for shredding (cross cut) or secure shreding receptables.
Hardcopy off site	Regular Trash	Shred or return to AVANGRID.	Shred or return to AVANGRID.	Return to AVANGRID.
Electronic data	None	None	Erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops to IT for appropriate disposal.	Erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops to IT for appropriate disposal.

6. Release to Third Party Vendors

Release to Third Party Vendors	Available to the general public and for distribution outside of AVANGRID.	Intended for use only within AVANGRID. May be shared with Third Party Vendors only if there is a legitimate business need to know and appropriate documentation has been obtained, e.g. data security rider, non-disclosure or confidentiality agreement, cyber insurance, back ground checks, etc.	Intended for use only within AVANGRID. May be shared with Third Party Vendors only if there is a legitimate business need to know and appropriate documentation has been obtained, e.g. data security rider, non-disclosure or confidentiality agreement, cyber insurance, back ground checks, etc.	Access limited to as few persons as possible on a need to know basis. Release only permitted if appropriate documentation has been obtained, e.g. data security rider, non-disclosure or confidentiality agreement, cyber insurance, back ground checks, etc., and approved by information/data owner (or custodian) and Corporate Security.