**ERCOT CORPORATE STANDARD**

|  |  |
| --- | --- |
| Document Name: | Information Protection Corporate Standard |
| Document ID: | CS7.6 |
| Effective Date: | December 10, 2021 |
| Owner: | General Counsel & Critical Infrastructure Security |
| Governs: | ERCOT Personnel |
| Approved: | Betty Day, VP Governance, Risk & Compliance |

# *Purpose*

The purpose of this corporate standard is to establish responsibility for Information Owners and Personnel to classify, label, and protect Information.

*See CP7 Security Corporate Policy for information pertaining to exceptions, violations, document management, and assistance with this corporate standard.*

# *Terms and Definitions*

|  |  |
| --- | --- |
| **Term**  | **Definition** |
| BES Cyber System Information | As defined in [Glossary of Terms Used in NERC Reliability Standards](https://www.nerc.com/files/glossary_of_terms.pdf) |
| CEII | Critical Energy Infrastructure Information pursuant to NERC Rules of Procedure Section 1500 |
| Information | Intellectual property and business Information created, received, used, processed, stored, maintained, or transmitted within the ERCOT environment. Information refers to ERCOT Information and information entrusted to ERCOT by 3rd parties without regard to form (website, electronic and hard copy documents and files, audio files, e-mail, input data, output data, and other materials.) |
| Information Owner | The ERCOT business unit or division responsible for determining the value, criticality, and management of ERCOT Information assets.  The Information Owner should delegate this responsibility to a designated Information Manager. |
| Personnel | Persons who need to access ERCOT facilities or systems, networks or information including:* ERCOT Employees and Contract Workers;
* Independent Market Monitor (IMM) employees and Contract Workers;
* Public Utility Commission of Texas staff members or Contract Workers;
* ERCOT Board of Directors members and Board Segment Alternates
 |
| PCII | Protected Critical Infrastructure Information pursuant to Department of Homeland Security rules |
| Personnel Records | Individual employees’ and employment candidates’ personal information such as contact information, social security numbers, driver license numbers, compensation rates, performance evaluations, disciplinary actions, and PHI. Included are records maintained in paper files, electronic files, candidate tracking systems, payroll systems, and HRIS systems. |
| PHI | Protected Health Information as defined by the Health Information Privacy and Protection Act. |

# *Information Classification*

Information falls within one of three classifications: **Public, ERCOT Internal,** and **ERCOT Confidential.** Information is classified according to the most sensitive details of the Information. The default classification for Information is **ERCOT** **Internal.**

## Public

Information officially released for public disclosure. Careful consideration should be given before classifying information as Public and releasing outside of ERCOT. Release of this information represents no to minimal risk.

## ERCOT Internal

Information intended for use within ERCOT and for which inadvertent access or disclosure represents a minimal risk.

## ERCOT Confidential

Information intended for very limited use within ERCOT and for which inadvertent access or disclosure represents at least moderate risk.

Information classified as **ERCOT Confidential** includes, but is not limited to:

* All BES Cyber System Information;
* All Information that is “Protected Information” or “ERCOT Critical Energy Infrastructure Information (ECEII)” under the ERCOT Protocols;
* Protected Critical Infrastructure Information (PCII); and
* Personnel Records.

BES Cyber System Information shall also be handled pursuant to a BES Cyber System Information protection program. [CIP-011-1 R1]

# *Reporting Improper Disclosure or Loss*

Disclosure of information other than BES Cyber System Information shall occur in accordance with the **GL 7.6.1: Information Classification Guideline**. Personnel must immediately notify General Counsel at disclosures@ercot.com regarding any known or suspected inadvertent or unauthorized disclosure or loss of Information classified as **ERCOT Internal** or **ERCOT Confidential.** Any requests for an exception to this corporate standard must be completed by contacting the General Counsel department at disclosures@ercot.com.

# *Roles and Responsibilities*

Critical Infrastructure Security and General Counsel are responsible for updating this corporate standard, supporting guideline [GL7.6.1] and BES Cyber System Information protection program.

Critical Infrastructure Security and General Counsel provide training for and ensure consistent communication to ERCOT Personnel regarding this corporate standard at least once every 15 calendar months.

Personnel are responsible for implementation of this corporate standard.

This corporate standard in no way limits other ERCOT standards, policies and procedures from requiring more specific notification requirements as mandated by regulatory or legal requirements.