ERCOT CORPORATE STANDARD

Document Name:	Information Protection Corporate Standard
Document ID:	CS7.6
Effective Date:	December 10, 2024
Owner:	Chad Seely, Sr. Vice President & General Counsel
Governs:	ERCOT Personnel
Approved:	Pablo Vegas, President & Chief Executive Officer

1. 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.

2. Terms and Definitions

Term	Definition
BES Cyber System Information	As defined in Glossary of Terms Used in NERC Reliability Standards and is also referred to as BCSI
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.

3. Information Classification

Information falls within one of three classifications: **Public, Internal, and Confidential. Confidential – BCSI is a sub-category of the Confidential** classification**.** Information is classified according to the most sensitive details of the Information. The default classification for Information is **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.

Internal

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

Confidential

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

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

- All BES Cyber System Information (BCSI);
- All ERCOT developed code;
- 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.

Any personnel seeking to reclassify Information classified as **Confidential** specified above in the bullets, may seek a Management Exception, in accordance with the

CS1.11 Management Exception Corporate Standard. A Management Exception to this corporate standard may only be approved by the signatures of IT, Compliance/Cyber Security, Corporate Communication, Area Officer(s), Legal, and the CEO or their delegate.

Confidential – BCSI

BES Cyber System Information (per NERC Reliability Standards) should be labeled as Confidential – BCSI. Authorization to access, reproduce or forward such information must always be obtained from the Information Owner. By default, information classified as BCSI is also considered Confidential and maintains the same security requirements in addition to those required under the BCSI category.

BES Cyber System Information shall also be handled pursuant to ERCOT's BES Cyber System Information Protection Program. [CIP-011-1 R1]

Confidential – ECEII

ERCOT Critical Energy Infrastructure Information (ECEII) should be labeled as Confidential – ECEII. When ECEII is submitted to ERCOT, it should already be labeled ECEII, per Protocol Section 1.3.2.2(1). However, ERCOT can designate unlabeled information ECEII, per Protocol Section 1.3.2(3). ERCOT, the IMM, or any Market Participant may not disclose ECEII to any other Entity except as specifically permitted in the Protocols, per Protocol Section 1.3.2(1).

Best practices when an exception allows sharing ECEII include taking reasonable steps to avoid public disclosure.

4. 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 **Internal** or **Confidential** (this includes **BCSI**). Any requests for an exception to this corporate standard must be completed by contacting the General Counsel department at disclosures@ercot.com.

5. 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. ECEII training is provided to New Hires, and Managers may request ECEII training to be assigned to their staff.

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.