MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 3.4: Activity - Data Classification Scheme: Hypothetical "SunPeak" Solar Power Substation

This data classification scheme outlines the classification levels for data handled at the SunPeak solar power substation, along with corresponding protection measures. The scheme is designed to manage risk effectively and ensure compliance with relevant regulations.

I. Classification Levels:

SunPeak will use a three-level classification scheme:

Public: Information that can be freely shared without risk to SunPeak's operations or security.

Internal: Information used internally within SunPeak; unauthorized access could cause operational disruption or minor financial losses.

Confidential: Information that requires the strictest protection; unauthorized access could cause significant operational disruption, financial losses, legal repercussions, or reputational damage.

II. Definition of Levels:

Public: This classification applies to information that does not pose a security or operational risk if disclosed. It may include general company information, marketing materials, and non-sensitive operational data.

Internal: This classification covers sensitive data used for internal operations. Unauthorized access could impact the efficiency of the substation or cause minor financial losses. Examples include employee schedules, internal memos, and some operational data (e.g., maintenance schedules for non-critical equipment).

Confidential: This classification is for highly sensitive data that requires the highest level of protection. Unauthorized access could have severe consequences, including significant financial loss, regulatory fines, legal action, and damage to the company's reputation. This includes data related to the SCADA system, grid connection details, financial records, customer contracts, and intellectual property.

III. Examples of Data at Each Level:

Classification Level	Data Examples
Public	Company website content, press releases, general operational information
Internal	Internal communications, employee training documents, non-critical maintenance logs
Confidential	SCADA system data, grid connection diagrams, financial reports, customer contracts, intellectual property

IV. Data Protection Measures:

Classification Level	Data Protection Measures
Public	Standard access controls, basic data backup
Internal	Network access controls, access control lists (ACLs), encryption at rest, regular data backups

Confidential	Strong encryption (both in transit and at rest), strict access control measures (including multi-factor authentication), regular security audits, robust incident response plan, comprehensive logging, intrusion detection and prevention systems

V. Policy Implementation:

- All data will be appropriately labeled with its classification level.
- Access to data will be granted based on the principle of least privilege.
- Regular audits and reviews will be conducted to ensure compliance.
- Employees will receive training on data classification and security best practices.
- The policy will be regularly reviewed and updated to reflect changes in the organization's operations and the threat landscape.

VI. Incident Response:

Any suspected or confirmed unauthorized access to confidential data will trigger the organization's incident response plan. This plan will outline steps for containment, eradication, recovery, and post-incident analysis.

This data classification scheme provides a framework for protecting sensitive information. It is crucial that employees are trained on this scheme, and that access controls and security measures are consistently implemented and regularly reviewed to maintain effectiveness. This is a hypothetical example; the SunPeak organization should consult with relevant legal and security experts to ensure its data classification scheme meets the requirements of all applicable laws and regulations.

This detailed example would be a suitable submission to the discussion panel, providing a starting point for further discussion and analysis of data classification and protection measures.