PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

FR 4 – Data Confidentiality

- FR1 – Identification, authentication and access control
- FR2 – Use Control
- FR3 – System Integrity
- FR4 – Data Confidentiality
- FR5 – Restrict Data Flow
- FR6 – Timely response to event
- FR7 – Resource Availability

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

PUBLIC

Data that can be freely shared with anyone

Examples:

- Directories
- Press releases
- Mission statements

INTERNAL

Data shared within the organization

Examples:

- Work schedules
- Budgets
- Project plans
- Strategies
- Business processes

CONFIDENTIAL

Data shared with select internal individuals as needed for their jobs

Examples:

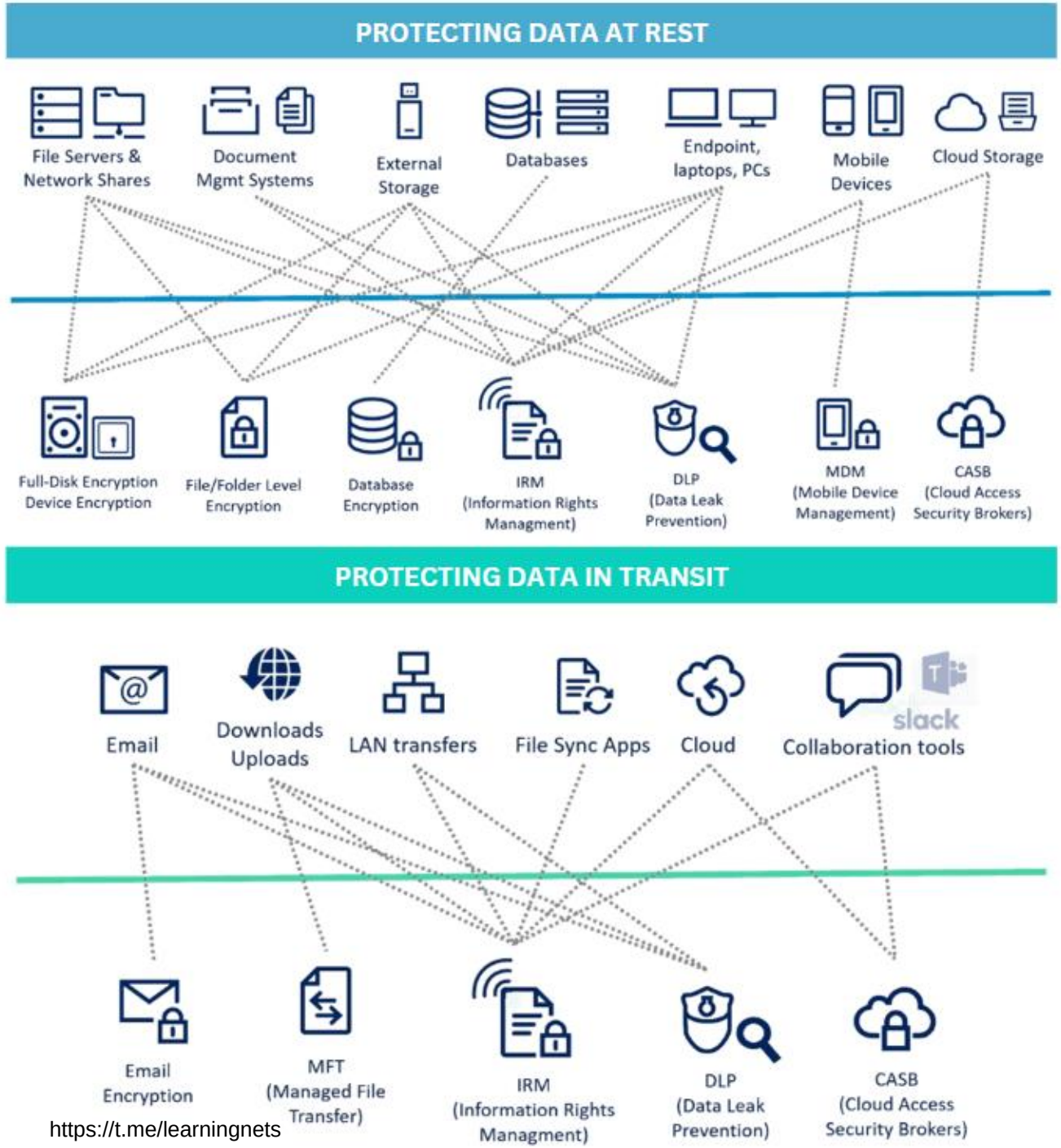
- Some regulated data (personal identifiable information, protected health information, HIPAA)
- Personnel records
- Financials

RESTRICTED

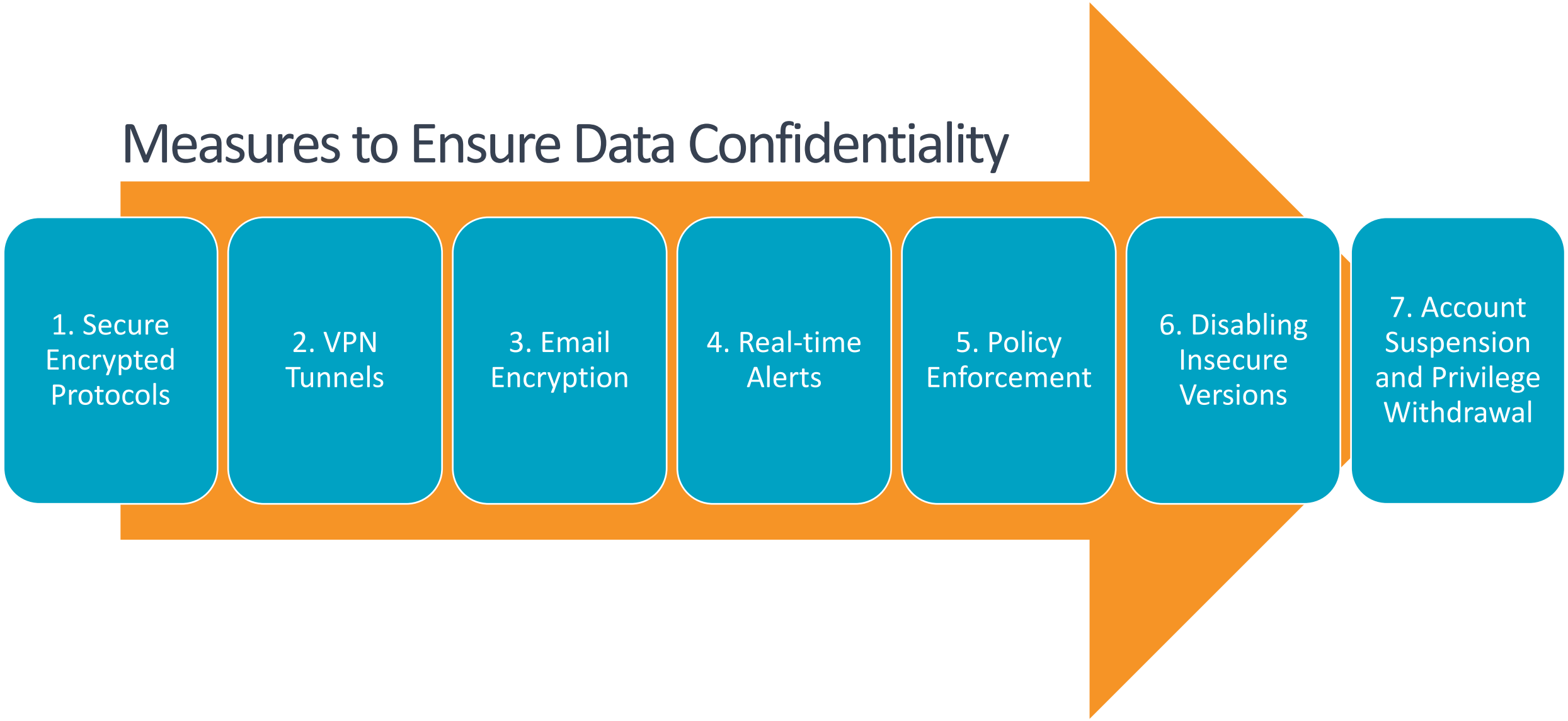
Data that is highly sensitive

Examples:

- Passwords
- Some highly regulated data
- Merger/acquisition plans
- Critical intellectual property



Measures to Ensure Data Confidentiality



Data Confidentiality as per IEC 62443 SL3 & SL4

- Restrict Access to Data
- Encrypt Data
- Implement a Confidentiality Policy
- Implement a Data Retention Policy
- Develop and Implement a Cyber Security Program
- Take Physical Security Measures

Implementing least privilege access control ensures confidentiality by granting authorized users minimal necessary permissions, minimizing risks of unauthorized disclosures or modifications, and limiting access to relevant data for their roles.

Restrict Access to Data

Encrypt Data

Implement a Confidentiality Policy

Implement a Data Retention Policy

Develop and Implement a Cyber Security Program

Take Physical Security Measures

Encryption ensures data confidentiality by converting information into unreadable form using complex algorithms, preventing unauthorized decryption and maintaining security in storage, communication, and transmission.

- Restrict Access to Data
- **Encrypt Data**
- Implement a Confidentiality Policy
- Implement a Data Retention Policy
- Develop and Implement a Cyber Security Program
- Take Physical Security Measures

A confidentiality policy is essential to secure data, guiding employees to handle sensitive information carefully through encrypted communication and secure practices, reducing the risk of unauthorized disclosure.

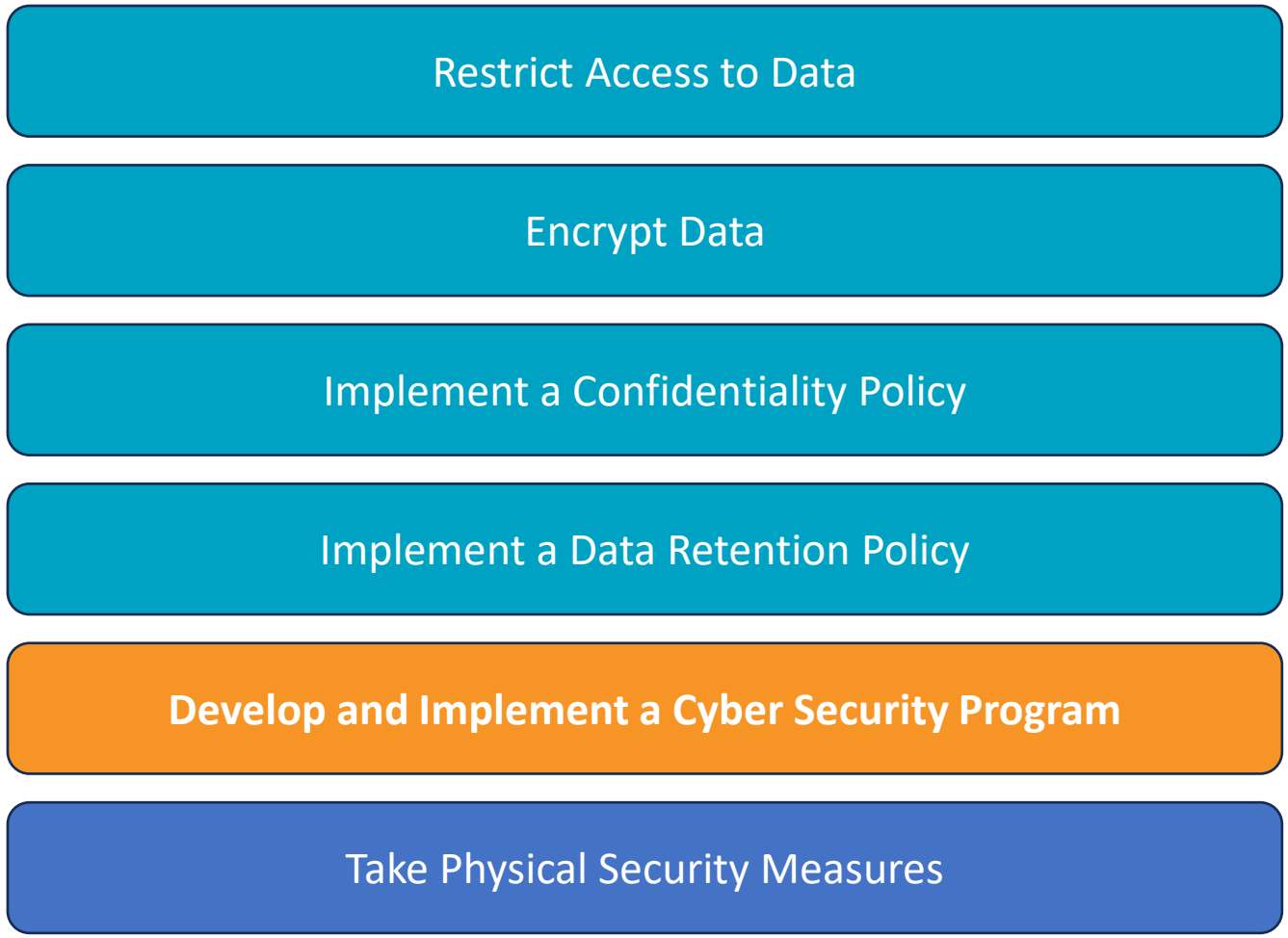
- Restrict Access to Data
- Encrypt Data
- **Implement a Confidentiality Policy**
- Implement a Data Retention Policy
- Develop and Implement a Cyber Security Program
- Take Physical Security Measures

Data retention and disposal policies are vital for effective data management and security. These policies determine how long data should be stored and how to securely dispose of it, based on business needs and compliance.

- Restrict Access to Data
- Encrypt Data
- Implement a Confidentiality Policy
- **Implement a Data Retention Policy**
- Develop and Implement a Cyber Security Program
- Take Physical Security Measures

Key components of a cybersecurity program include:

1. Risk Assessment
2. Data Protection Measures:
3. Physical Security
4. Security Policies and Procedures:
5. Incident Response Plan
6. Employee Training
7. Regular Monitoring and Auditing:
8. Updates and Patches
9. Vendor and Third-Party Management



Safeguarding data involves cyber and physical security measures; implementing office alarms, surveillance, access controls, and monitoring enhances protection against theft and unauthorized access, providing a comprehensive approach to data security.

- Restrict Access to Data
- Encrypt Data
- Implement a Confidentiality Policy
- Implement a Data Retention Policy
- Develop and Implement a Cyber Security Program
- **Take Physical Security Measures**

Wrap Up

- Data confidentiality is vital for organizations to protect sensitive information and uphold trust.
- Implementing encryption, data classification, confidentiality policies, data retention policies, cybersecurity programs, and physical security measures enhances data confidentiality.
- These measures help prevent unauthorized access or disclosures of sensitive data.
- Prioritizing data confidentiality is crucial for overall security and maintaining trust with stakeholders.