

	<b>Standard</b>	<b>Generation Engineering</b>
---	-----------------	-------------------------------

Title: **Data and Information Security in Power Plant Operations Standard**

Unique Identifier:

**240-82332463**

Alternative Reference Number:

**N/A**

Area of Applicability:

**Engineering**

Documentation Type:

**Standard**

Revision:

**1**

Total Pages:

**18**

APPROVED FOR AUTHORISATION  
☒ GENERATION ENGINEERING  
DOCUMENT CENTRE ☎ x4962

Next Review Date:

**March 2028**

Disclosure Classification:

**CONTROLLED  
DISCLOURE**

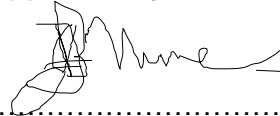
**Compiled by**



**Dr. Craig D. Boesack**  
**Chief Engineer, Generation Engineering**

Date: 22/03/2023

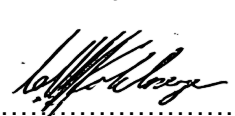
**Approved by**



**Jorge Nunes**  
**Chief Engineer, Generation Engineering**

Date: 2023/03/22


**Authorised by**



**Christoph Kohlmeyer**  
**Senior Manager, C&I CoE (Acting)**

Date: 2023-03-22

**Supported by SCOT SC**



**Dr. Craig D. Boesack**  
**SCOT SC Chairperson**

Date: 22/03/2023

PCM Reference : **240-56355828**

SCOT Study Committee Number/Name : **Power Plant Study Committee, PP C&I SC08-03**

## **CONTENTS**

	<b>Page</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>1. INTRODUCTION .....</b>	<b>4</b>
<b>2. SUPPORTING CLAUSES .....</b>	<b>4</b>
2.1 SCOPE .....	4
2.2 NORMATIVE/INFORMATIVE REFERENCES .....	4
2.3 DEFINITIONS .....	5
2.4 ABBREVIATIONS .....	6
2.5 ROLES AND RESPONSIBILITIES .....	6
2.6 PROCESS FOR MONITORING .....	6
2.7 RELATED/SUPPORTING DOCUMENTS .....	6
<b>3. MANAGING DATA SECURITY FOR OPERATIONAL TECHNOLOGY .....</b>	<b>7</b>
3.1 GOVERNANCE OF DATA AND INFORMATION SECURITY .....	7
3.2 SECURITY REQUIREMENTS .....	7
3.3 DATA AND INFORMATION SECURITY REQUIREMENTS FOR POWER PLANT CONTROL SYSTEMS (DCS, PLC, SCADA) .....	9
3.4 REQUIREMENTS FOR PROTECTING SENSITIVE DATA IN POWER PLANT CONTROL SYSTEMS .....	9
3.5 DOCUMENT AND DATA CLASSIFICATION .....	10
3.6 MANAGING CYBER RISK RELATING TO OT SENSITIVE INFORMATION .....	10
3.7 DATA LIFE CYCLE MANAGEMENT .....	11
3.8 THE INFORMATION SECURITY MODEL .....	11
3.9 INFORMATION CHARACTERISTICS .....	12
3.10 INFORMATION STATES .....	13
3.11 SECURITY COUNTERMEASURES .....	14
<b>4. DATA CREATION, STORAGE AND BACKUP .....</b>	<b>15</b>
4.1 DATA CREATION .....	15
4.2 STORAGE AND BACKUP .....	15
<b>5. RISK ASSESSMENT .....</b>	<b>16</b>
<b>6. PRESENT DATA IN A SECURE &amp; PROTECTED WAY .....</b>	<b>17</b>
<b>7. AUTHORISATION .....</b>	<b>18</b>
<b>8. REVISIONS .....</b>	<b>18</b>
<b>9. DEVELOPMENT TEAM .....</b>	<b>18</b>
<b>10. ACKNOWLEDGEMENTS .....</b>	<b>18</b>

## **FIGURES**

Figure 1 – The McCumber Information Security Model.....	12
---	----

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **EXECUTIVE SUMMARY**

The secure handling of sensitive operational technology (OT) data is crucial for power plant operations. Unauthorized disclosure, loss, damage, or modification of sensitive OT documents can have severe consequences.

Therefore, all sensitive information must be treated with the utmost confidentiality, and integrated security measures must be put in place to safeguard against potential breaches.

It is imperative to prioritize data and information security in power plant operations to ensure the safe, efficient, and uninterrupted functioning of the power plant facility.

## **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **1. INTRODUCTION**

The purpose of this document is to raise awareness of data governance in Operational Technology (OT) and emphasize the importance of protecting sensitive OT data from corruption while ensuring its accessibility. As OT becomes increasingly integral to modern industrial processes, it is crucial to understand the significance of maintaining data security.

This document also highlights the need for implementing effective data protection technologies and best practices to safeguard sensitive OT information against potential breaches. By prioritizing data governance, organizations can maintain the reliability and efficiency of their OT systems while safeguarding against data loss or unauthorized access.

## **2. SUPPORTING CLAUSES**

### **2.1 SCOPE**

The scope of this standard is to establish guidelines for maintaining data and information security in power plants, specifically within Operational Technology (OT) systems.

1. The standard covers all systems, including control system networks, servers, networked equipment, and devices that handle sensitive OT information.
2. The document provides guidance on data classification, managing cybersecurity risks related to sensitive OT data, data protection, information distribution, and lifecycle management.
3. The standard aims to ensure the confidentiality, integrity, and availability of OT data while minimizing the risks associated with unauthorized access or data breaches.
4. By adhering to this standard, power plant operators can enhance the security and reliability of their OT systems and minimize the potential impact of cybersecurity threats.

#### **2.1.1 Purpose**

The purpose of this document is to emphasize the importance of maintaining robust data and information security measures for sensitive information within Operational Technology (OT) systems in power plants.

The document aims to establish organizational standards and best practices for protecting sensitive information by outlining necessary controls that ensure appropriate levels of protection.

By prioritizing data and information security, power plant operators can minimize the risks associated with unauthorized access, data breaches, and other cybersecurity threats, while ensuring that sensitive OT information remains confidential, intact, and available only to authorized personnel.

#### **2.1.2 Applicability**

This standard is applicable to Generation.

## **2.2 NORMATIVE/INFORMATIVE REFERENCES**

### **2.2.1 Normative**

- |     |        |  |
|-----|--------|--|
| [1] | 32-438 | Information Security Systems Classification Standard |
| [2] | 32-85  | Information Security Policy                          |
| [3] | 32-351 | Eskom Integrated Risk Management Policy              |

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

[4] 240-55410927 Cyber Security Standard for Operational Technology

[5] 240-129014618 Generation Cyber Security Guideline

### 2.2.2 Informative

[6] ISO 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements.

[7] NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments.

[8] ISA/IEC 62443 Security for Industrial Automation and Control Systems

[9] IEC 62351 Power Systems Management and Associated Information Exchange – Data and Communication Security

## 2.3 DEFINITIONS

Definition	Description
Access Control	Security mechanisms and policies that restrict access to sensitive information within OT systems to only authorized personnel.
Cybersecurity Risk Management	The process of identifying, assessing, and prioritizing potential cybersecurity risks within OT systems, and developing and implementing strategies to mitigate those risks.
Data Classification	The process of categorizing data based on its level of sensitivity to ensure that appropriate security measures are applied to protect it.
Data Security	Data security means protecting digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or a data breach. (source: Wikipedia)
Encryption	The process of converting plain text into cipher text using a mathematical algorithm, making it unreadable to anyone without the key to decrypt it. Encryption is often used to protect sensitive data in transit or at rest.
Incident Response Plan	A documented procedure outlining the steps to be taken in the event of a cybersecurity incident or data breach, with the goal of minimizing the impact of the incident and restoring normal operations as quickly as possible.
Operational Technology (OT)	Refers to hardware and software technologies used in industrial control systems that manage and monitor industrial processes, including power plant operations.
Vulnerability Assessment	The process of identifying and evaluating potential weaknesses in OT systems that could be exploited by cyber attackers to gain unauthorized access to sensitive information.

### 2.3.1 Disclosure Classification

**Controlled Disclosure:** Controlled Disclosure to external parties (either enforced by law, or discretionary).

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **2.4 ABBREVIATIONS**

<b>Abbreviation</b>	<b>Description</b>
OT	Operational Technology
BU	Business Unit
DCS	Distributed Control System
PLC	Programmable Control System
SCADA	Supervisory Control and Data Acquisition
Gx	Generation Division
IT	Information Technology
OEM	Original Equipment Manufacturer
CIA	Confidentiality, Integrity, and Availability
AAA	Authentication, Authorization and Accounting
SIEM	Security Information and Event Management
IP	Internet Protocol
C&I	Control and Instrumentation
SC	Study Committee

## **2.5 ROLES AND RESPONSIBILITIES**

The implementation of the standard is the accountability of the Eskom Generation Business Unit (BU) or System Owner. The BU or System Owner may delegate the responsibility of the implementation, the management, and the support necessary to facilitate standard implementation.

## **2.6 PROCESS FOR MONITORING**

This document will be periodically reviewed and updated as necessary to reflect evolving technology and to align with the latest technology strategies based on business requirements.

## **2.7 RELATED/SUPPORTING DOCUMENTS**

None.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **3. MANAGING DATA SECURITY FOR OPERATIONAL TECHNOLOGY**

#### **3.1 GOVERNANCE OF DATA AND INFORMATION SECURITY**

Effective governance of data and information security is essential for ensuring the safe and reliable operation of power plants. In complementing the Generation Cybersecurity program, this section outlines the key principles for governing data security within Operational Technology (OT).

To effectively manage risks related to data security in OT, it is essential to make informed decisions based on a thorough understanding of the risks and potential impacts. This involves conducting regular risk assessments to identify potential vulnerabilities and threats and implementing appropriate security controls to mitigate those risks.

Clear roles and responsibilities must also be defined to ensure accountability for data security. This includes designating individuals or teams responsible for overseeing data security within OT systems, and establishing policies and procedures for data access, use, and protection.

Allocating appropriate resources to support data security within OT is crucial. This includes investing in security technologies and tools, providing ongoing training and education for personnel, and ensuring that adequate resources are allocated to support the ongoing monitoring and management of data security risks.

By following these principles for governing data and information security within OT, power plant operators can better protect their digital assets and ensure the safe and reliable operation of their facilities.

The following are key points regarding data and information security for power plants:

- a) Generation OT shall apply governance and management controls to protect data security.
- b) Information and data security is an enterprise issue managed throughout the entire Eskom organization.
- c) The cybersecurity program includes people, processes, procedures, systems, technologies, networks, and information across the horizontal, vertical, and cross-functional value chains of the Eskom business.
- d) OT engineering, maintenance, and operational departments shall regularly promote a culture of cybersecurity awareness and best practices.
- e) Senior management shall provide oversight of the cybersecurity program and allocate adequate resources to support its implementation.
- f) Senior management shall accept responsibility for security risks associated with their digital assets.
- g) Qualified personnel shall be assigned security roles and responsibilities, such as qualified system administrators.

#### **3.2 SECURITY REQUIREMENTS**

##### **3.2.1 Physical Security Requirements**

- a) The power plant control systems (DCS, PLC, and associated data and information) shall be physically protected by access control measures such as security cameras, biometric identification, and physical barriers.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

- b) The physical security measures shall be designed to prevent unauthorized access, tampering, damage, or theft of the control systems and associated data and information.
- c) The power plant control systems shall be located in secure areas with restricted access and limited entry points.
- d) All entry and exit points to the control system areas shall be monitored and controlled by authorized personnel.
- e) The control system areas shall have secure storage areas for any sensitive information, including passwords, cryptographic keys, and other access control mechanisms.
- f) Physical access to the control system areas shall be logged and monitored in real-time to detect any unauthorized access or suspicious activity.
- g) Any identified security breaches shall be immediately reported to the appropriate personnel for investigation and resolution.

### **3.2.2 Network Security Requirements**

- a) The power plant control systems shall be protected by secure network architecture that isolates control systems from non-control systems and external networks.
- b) The network security measures shall be designed to prevent unauthorized access, tampering, damage, or theft of the control systems and associated data and information.
- c) Network connections to the control systems shall be secured using encryption and authentication mechanisms to prevent unauthorized access or data interception.
- d) The control system network shall have intrusion detection and prevention mechanisms to detect and prevent any suspicious network activity.
- e) Network access to the control systems shall be restricted to authorized personnel only.
- f) All network activity related to the control systems shall be logged and monitored in real-time to detect any suspicious network activity or unauthorized access attempts.
- g) Any identified network security breaches shall be immediately reported to the appropriate personnel for investigation and resolution.

### **3.2.3 Access Control Requirements:**

- a) Access to the power plant control systems (DCS, PLC, and associated data and information) shall be restricted to authorized personnel only.
- b) Access control mechanisms shall be implemented to ensure that only authorized personnel have access to the control systems and associated data and information.
- c) Access control mechanisms shall include authentication, authorization, and accounting measures to ensure that access to the control systems is traceable and auditable.
- d) Passwords and other access credentials shall be managed in a secure manner, and users shall be required to change their passwords at regular intervals.

**CONTROLLED DISCLOSURE**



- e) Access to the control systems shall be granted on a need-to-know basis, and access permissions shall be reviewed and updated regularly to ensure that only authorized personnel have access.
- f) The control systems shall have mechanisms to detect and prevent unauthorized access attempts, including password guessing, brute-force attacks, and other unauthorized access methods.
- g) Any identified access control breaches shall be immediately reported to the appropriate personnel for investigation and resolution.

### **3.3 DATA AND INFORMATION SECURITY REQUIREMENTS FOR POWER PLANT CONTROL SYSTEMS (DCS, PLC, SCADA)**

- a) Data security for power plant control systems, including DCS, PLC, and SCADA systems, shall be maintained to ensure the confidentiality, integrity, and availability of data.
- b) OTs shall have the necessary security architecture and incident response plans in place to mitigate any security threats, including unauthorized access and disclosure of sensitive information.
- c) A data breach can have far-reaching operational, financial, and reputational impacts on the business, making better OT data security governance paramount.
- d) Therefore, data protection shall cover a broad spectrum of Gx business operations, including but not limited to Backup and Restore, Disaster Recovery, Business Continuity, System Availability, Cyber Security, Data Security, Data Protection Technologies, Governance & Compliance, and Information Lifecycle Management.
- e) All the elements mentioned above shall form part of a comprehensive data protection framework. The framework shall define how these elements interact to provide effective data protection for the business.

### **3.4 REQUIREMENTS FOR PROTECTING SENSITIVE DATA IN POWER PLANT CONTROL SYSTEMS**

- a) Data protection technologies shall be included in the data protection framework of the control system technology (DCS, PLC or SCADA), but data protection shall encompass a systematic process of policy, process and strategy, procedures, and practices.
- b) Protecting sensitive data within power plant control systems, including DCS, PLC, and SCADA, shall be a necessary requirement to avoid unpleasant consequences in the event of a data breach or compromise to either an OT or an enterprise system.
- c) The protection of sensitive information shall play a significant role in business continuity. The convergence of OT with IT has increased the ability to share, store, and transmit sensitive data across computer systems.
- d) Therefore, OT shall ensure that appropriate protective measures are in place to safeguard the confidentiality of sensitive information and data.
- e) Protecting sensitive data shall require a combination of people, processes, policies, and technologies, especially when handling and managing electronic documents and information.
- f) All OT personnel involved in operational, maintenance, and engineering responsibilities shall play a collective role in protecting sensitive data.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **3.5 DOCUMENT AND DATA CLASSIFICATION**

Managing the security of OT-sensitive data and information is of paramount importance. At some point in their work, personnel working with Operational Technology will deal with sensitive information, that is, information that requires a level of confidentiality.

Therefore, managing data security for Operational Technology requires appropriate levels of protection against unauthorised access or unauthorized disclosure or modification of data.

- a) All documents may be considered sensitive, even if documents are in draft format. Therefore, as a minimum, documents shall be classified at Confidential until their classifications are confirmed.
- b) Sensitive documents shall be always protected. Sensitive documents including both documents in electronic formats and documents in hardcopy form shall be protected and managed securely.
- c) The Information Security Systems Classification Standard (32-438) shall be used to define document classifications.
- d) Inappropriate disclosure of sensitive information can place the Generation business, its operations, and personnel at risk. Therefore, to mitigate these risks, all documents forming part of OT systems (i.e., sensitive information) shall be classified by following a formal classification process.
- e) Documents created by Gx OT or received from third parties (such as OEM) shall be classified under the expectation of confidentiality, these documents shall also follow a data classification process.

### **3.6 MANAGING CYBER RISK RELATING TO OT SENSITIVE INFORMATION**

- a) Data or Information Security Strategies, Risk Mitigation and Business Continuity:
  - i. A risk management approach shall be followed in the mitigation of cybersecurity risk. As part of the risk mitigation process, sensitive information shall be protected and classified at levels appropriate to mitigate risk.
  - ii. As a subset of risk management is business continuity and the requirements to ensure the protection of systems to mitigate risk and the consequences of system interruption because of inadequate document classification shall be considered as part of the risk assessment and document classification process.
  - iii. Data and information and the OT or IT infrastructure supporting information systems shall be protected at levels as defined by risk assessment and support the overall business continuity objectives.
- b) To ensure adequate data information security, all systems forming part of business continuity requires a software and hardware infrastructure where essential applications shall be available at all times. In the case of systems failure, the focus shall be given to minimising the impact on business continuity.
- c) There is a relationship between data protection, risk assessment and business continuity. Failure to protect data adequately could lead to business continuity concerns.
- d) Managing the security of Technical Documentation

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

All documents containing cybersecurity information shall be protected, these include but are not limited to:

- Network Diagrams or Plans
  - Cybersecurity Plans
  - Sensitive Information of Systems, Applications and Mission Critical documentation.
  - System Configuration, Data and Libraries
  - Systems Specifications (including drawings, plans, and equipment specifications)
  - Cybersecurity Risk Assessments, Vulnerability Assessments and Reports
- e) An approach based on a “need to know” basis shall be followed when disseminating information.
- f) A determination shall be made by the authorized system administrator of the documentation to ensure authorized access to information by prospective recipients of information.

### **3.7 DATA LIFE CYCLE MANAGEMENT**

- a) Data and Information Life Cycle Management shall be a policy-driven management process of information throughout its lifecycle, from conception to active life and disposition of information.
- b) Managing the mechanisms of storage infrastructure and data throughout its lifecycle shall be critical for data protection and business continuity in power plant control systems such as DCS, PLC, and SCADA.
- c) Data changes occur at different times throughout its life, reflecting a change process.
- Therefore, OT shall keep records of all changes to OT data to ensure the integrity of the data.
  - This shall include an understanding of the underlying content of the data, where data becomes information, and system administrators shall keep records of this knowledge.
- d) Data and information shall be classified based on their importance and sensitivity to the organization, and appropriate security controls shall be put in place to protect the data and information throughout their lifecycle.
- e) The data shall be regularly backed up and stored securely, and access control shall be implemented to ensure that only authorized personnel have access to the data and information.
- f) Finally, data and information shall be disposed of in a secure and responsible manner at the end of their lifecycle, following applicable legal and regulatory requirements.

### **3.8 THE INFORMATION SECURITY MODEL**

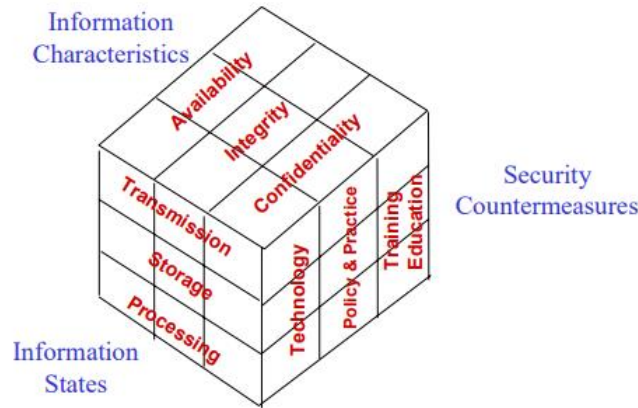
Some measures are described below that form part of protecting sensitive information and data for OT (or IT) systems (Figure 1).

Figure 1 shows the McCumber Model, a concise representation of information systems security and provides a framework for information assurance.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Protecting sensitive information and systems against unauthorized access to or modification of information, where information is in storage, processing, or in transit, it is necessary to detect, document and counter present or emerging threats.



**Figure 1 – The McCumber Information Security Model**

### **3.9 INFORMATION CHARACTERISTICS**

Protecting sensitive information is a multidisciplinary area of Confidentiality, Integrity, and Availability (CIA).

#### **3.9.1 Confidentiality**

- Confidentiality is the “assurance that information is not disclosed to unauthorized persons, processes or devices”.
- To apply this, information shall be classified (see the section on Document and Data Classification) and an approach based on a “need to know” basis shall be followed.
- Only authorised users/systems or resources shall view, access, change or otherwise use data.

#### **3.9.2 Integrity**

- Integrity is, “The quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.”
- Aspects of data integrity include:
  - A protection against unauthorized modification or destruction of information.
  - Data Integrity is also a matter of degrees of trust, elements of accuracy, relevancy, and completeness. The accuracy, consistency and trustworthiness of data shall be preserved.
  - Data and system integrity implies robustness.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **3.9.3 Availability**

According to the McCumber Model, Availability is a critical component of data and information security for power plant control systems, such as DCS, PLC, and SCADA.

- a) To ensure the availability of data and information, power plant operators shall implement appropriate measures such as redundancy and failover mechanisms, backups, and disaster recovery plans.
- b) Access controls shall be established to ensure that only authorized personnel have access to the data and information, and that any changes made to the systems are tracked and audited.
- c) In addition, all changes to the data shall be recorded, and assurance shall be given to the integrity of the data.
- d) System administrators shall keep records of the underlying content of the data, where data becomes information.
- e) Regular testing and evaluation of these measures shall be conducted to ensure their effectiveness and to identify any potential vulnerabilities that could compromise the availability of data and information.
- f) The consequence of failing to ensure availability can be severe, including loss of control over critical systems, equipment failure, and hazardous situations.

## **3.10 INFORMATION STATES**

Information can be found in one or more states, namely, Stored, Processed or Transmitted.

### **3.10.1 Transmission**

- a) OT data shall be transmitted in a secure manner using encryption and authentication mechanisms to ensure confidentiality and integrity of the data during transit.
- b) Access control measures shall be implemented to prevent unauthorized access to the data during transmission.

### **3.10.2 Storage**

- a) OT data shall be stored in a secure and reliable manner to ensure its confidentiality, integrity, and availability.
- b) Access to the stored data shall be restricted to authorized personnel only, and appropriate backup and recovery mechanisms shall be put in place to ensure the availability of the data in case of a disaster or system failure.

### **3.10.3 Processing**

- a) OT data shall be processed in a secure manner to ensure its confidentiality, integrity, and availability.
- b) Access to the processing systems shall be restricted to authorized personnel only, and appropriate monitoring mechanisms shall be put in place to detect any unauthorized access or activity.
- c) In addition, data processing activities shall be audited and logged to provide a traceable record of all transactions.

## **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **3.11 SECURITY COUNTERMEASURES**

Confidentiality is breached when an unauthorized entity can view, take and/or change OT (or organizational data).

Therefore, to prevent unauthorized access there are several mechanisms and controls which can be applied to data to protect the Confidentiality, Integrity and Availability of data.

These are listed below, but are not only limited to these:

- a) **User Access Controls** - Shall govern each user's ability to read, execute, change, or delete information associated with an OT computer system resource.
  - The system administrator shall be responsible for granting access or denying the ability of users to interact with a resource, including access to information, access to systems, or other activities that may be performed relating to the OT resource.
  - The access control system shall be integrated with the operating system, such as PLC, DCS, or SCADA systems, or part of a more general resource management and control environment, such as document control, change, or modification management.
  - Access Control methods used within the industry shall include, but not limited to, the following:
    - Role-Based Access Control shall enforce access control based on a user's role, which may be specific to the organization, function of a user within the organizational structure, or linked to job titles.
    - Discretionary Access Control shall allocate access to users based on a "need to know" basis, and the system administrator shall be responsible for it.
  - The AAA Model, which stands for Authentication, Authorization, and Accounting, shall be a security framework that controls access to computer resources and enforces policies. AAA shall play a role in network management and cybersecurity by screening users and keeping track of their activity.
- b) **Password policies** - Password policies shall be implemented to ensure that users create strong passwords and change them regularly. Passwords shall be protected during transmission and storage to prevent unauthorized access.
- c) **Two-factor authentication** - To increase security, two-factor authentication shall be implemented where possible. This could include the use of smart cards, tokens, or biometric identification.
- d) **Audit trails** - An audit trail shall be maintained to track user activity, including logins, logouts, and changes made to the system. This information can be used to detect and investigate security incidents.
- e) **Separation of duties** - The principle of separation of duties shall be implemented to prevent any one user from having too much control or influence over the system. This could involve assigning different roles and responsibilities to different users and implementing appropriate access controls to limit their access to certain areas of the system.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.



- f) **Monitoring** - The access control system shall be regularly monitored to detect any unauthorized access attempts or suspicious activity. This could involve the use of intrusion detection systems, security information and event management (SIEM) systems, and other monitoring tools.

#### **4. DATA CREATION, STORAGE AND BACKUP**

There are several supporting technologies used to enhance the security of data, data protection and associated information for OT systems.

Starting with the basics of Data Creation, Storage and Backup, the following discourse seeks to characterize the various data protection technologies.

##### **4.1 DATA CREATION**

- a) System administrators shall ensure that PLC, DCS & SCADA systems are protected by using the inherent data protection mechanisms and tools of the systems, such as disk encryption, user access control, authentication, and accounting, to safeguard sensitive information that is created, stored, and backed up as part of the system infrastructure, including system-generated data and production or engineering data.
- b) The creation of data and data protection technologies forming part of the PLC, DCS & SCADA systems shall be engineered for Confidentiality, Integrity, and Availability (CIA).
- c) The system administrator shall ensure that data protection mechanisms for PLC, DCS & SCADA systems are varied in terms of the levels of protection, depending on the capability of the technology employed.
- d) If PLC, DCS & SCADA systems have limited data protection mechanisms built into the system, the system administrator shall perform the data protection function to ensure the confidentiality, integrity, and availability of sensitive information.

##### **4.2 STORAGE AND BACKUP**

Storage and backup are critical components of data and information protection. In order to ensure the integrity and availability of data, the following shall be implemented:

- a) All OT data shall be stored on secure and reliable storage media, with adequate capacity for the intended purpose.
- b) OT data shall be backed up regularly, with backups stored in secure locations, to ensure availability in the event of system failures, disasters or cyber-attacks.
- c) Backup and storage systems shall be tested periodically, to verify that they are functioning as intended, and to identify any potential issues.
- d) Backup and storage systems shall be designed with redundancy, to ensure that data can be recovered in the event of hardware or software failures.
- e) The retention period for backup data shall be defined by the system administrator, considering the regulatory requirements and the business needs.
- f) All backup data shall be secured using the same level of protection as the original data, including access controls, encryption, and other appropriate security measures.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **5. RISK ASSESSMENT**

- a) Risk assessment forms a baseline to assess risks, from which the security posture within OT can be improved.
- b) The process of identifying and prioritizing risks shall be clearly documented by OT (i.e., the system administrator of the specific power plant shall perform this function).
- c) Part of the risk assessment process shall incorporate threat and vulnerability analysis and shall provide the necessary security controls to mitigate each risk as contained within the risk assessment.
- d) When considering the OT-specific threats to critical infrastructure and assets, from the perspective of Data Integrity, the following risk factors shall be considered (but not limited to the following):
  - Insider threats
  - Malware
  - Compromise of trusted systems
  - Vulnerabilities due to unpatched or obsolete systems
  - Poor access control
  - Modification or deletion of OT assets
  - The negative impact on business operations or reputation.
- e) In managing data or information security risk, the focus shall be given to the impact on business operations, OT and IT impact and business continuity.
- f) The impact on system functions, the accuracy of data availability and the risk relating to data integrity shall be assessed.
- g) Compromised data integrity means a loss of confidentiality and harm from unauthorized access or alteration of data. Therefore, increased focus shall be given to the data integrity of systems during risk assessment evaluations.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.



## **6. PRESENT DATA IN A SECURE & PROTECTED WAY**

Data shall be always presented in a secure and protected way, with a conservative approach recommended as follows:

Data and information shall be presented in a secure and protected way to ensure the safety and reliability of the plant's operation.

This means that access to data and information must be restricted to authorized personnel only and protected against unauthorized access, alteration, or destruction. To achieve this, various security measures shall be employed, such as encryption, user access controls, authentication, and accounting.

It is also important to maintain backups of critical data to ensure the continuity of operations in the event of a system failure or cyber-attack.

- a) All Third Parties (External Stakeholders, Auditors or OEM/Vendors) provided with confidential information shall individually sign the Declaration of Secrecy form (SD/SBI-0006008) in compliance with Eskom's Cyber Security governance.
- b) If Third Parties (External Stakeholders, Auditors or OEM/Vendors) request sensitive documents, only the cover page (Doc number hidden) including the document index shall be shared to demonstrate the existence, scope, authorization, and date of the relevant documents.
- c) Network architectures, IP addresses, usernames, passwords, and critical cyber asset lists shall not be shared.
- d) Third Parties (External Stakeholders, Auditors or OEM/Vendors) shall not install any third-party software (on OT computer systems).
- e) Remote audits are not recommended. Instead, Third Parties (External Stakeholders, Auditors or OEM/Vendors) should come to the site for compliance explanation and demonstration, but no screen shots or photos shall be allowed.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## 7. AUTHORISATION

This document has been seen and accepted by:

<b>Name &amp; Surname</b>	<b>Designation</b>
Christoph Kohlmeyer	Chief Engineer
Cornelius Visagie	Chief Technologist
Craig D. Boesack	Chief Engineer
Isaac Sibiya	Chief Technologist
Jorge Nunes	Chief Engineer
Thokozani Msibi	Chief Engineer
Felix Bosch	Generation Engineering Document Manager

## 8. REVISIONS

<b>Date</b>	<b>Rev.</b>	<b>Compiler</b>	<b>Remarks</b>
07/07/2022	0.0	CD Boesack	First Draft for Comments Review Process
March 2023	0.1	CD Boesack	Final Draft after Comments Review Process
March 2023	1	CD Boesack	Final Document for Authorisation and Publication

## 9. DEVELOPMENT TEAM

The following people were involved in the development of this document:

1. Jorge Nunes
2. Christoph Kohlmeyer
3. Control System Care Group Members.
4. Review and acceptance by the C&I SC.

## 10. ACKNOWLEDGEMENTS

The Control System Care Group Members are thanked for their contributions to the development of this document.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.