Esko Digital Information Security
Technical, Administrative, Physical and Organizational Measures v2023
(last update : 10 November 2023)

## Esko Digital Information Security - Definition

Digital Information Security at Esko means guaranteeing the confidentiality, integrity, availability, and compliance of all corporate information stored, processed, transported and represented by IT systems under the control and responsibility of Esko in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities.

## Esko Digital Information Security - Purpose

Protecting Esko Data is critical to the reputation, operation, and financial well-being of Esko. Effective security controls must be in place to protect Esko information and Esko IT Assets, and the business processes they support, against accidental or intentional unauthorized use, disclosure, transfer, modification, or destruction. These security controls must meet business, legal, regulatory, and compliance requirements and support the Esko Shared Purpose and core values – Safeguarding the World's Most Vital Resources™

## Esko Digital Information Security - Scope

The Esko Digital Information Security applies to Esko, associates, contingent workers, contractors, vendors, service providers, consultants, and authorized agents of Esko using or accessing Esko Data and/or Esko IT Assets; hereto referred to as "users." The Esko Digital Information Security also applies to systems owned by Esko and affiliates whether located on-premises or at off-site locations (i.e., hosted internally or cloud-based).

Esko has the obligation to meet applicable business, legal, regulatory and compliance requirements to protect its Data and its IT Assets. Esko also has a duty to protect all users against security threats and vulnerabilities.

## Esko Digital Information Security - Technical, Administrative, Physical & Organizational Measures (in general)

# 1 Digital Information Security Program

### 1.1 Program Governance & Responsibilities

a) The Esko Digital Information Security Program is directed by Esko Security team which is led by the Esko Chief Information Security Officer (CISO). Esko Security is responsible for the vision, mission and objectives delivered to Esko to enable appropriate and reasonable protection of Esko Data and Esko IT Assets across the organization. Esko Security team will work closely with Esko leadership to align and coordinate the execution of the security vision, mission, objectives, and services.

b) The CISO maintains an Esko Global Security Council (EGSC) meeting to ensure alignment, prioritization, understanding and management of information security risks.

c) Digital Information Security is a shared responsibility at Esko. Esko Security team works with Esko leadership to ensure effective and timely implementation of Esko Digital Information Security through alignment with business priorities and following a risk-based approach.

d) Esko CIO is responsible for ensuring that the Esko Digital Information Security actions and controls are carried out within Esko. Esko CIO is also responsible for ensuring that users are aware of Esko policies and procedures related to IT security.

### 1.2 Digital Information Security Coordination

Digital Information Security coordination is performed by the Esko Security team and the implementation occurs in conjunction with Esko leadership. A Digital Information Security Program is maintained and monitored through the following:

a) Developing, reviewing and approving the Esko Digital Information Security Policy (including any companion and/or supplemental policies) and overall responsibilities;

b) Performing risk assessments and accompanying risk mitigation and management strategies;

c) Communication and reporting via dashboards, metrics, and bowlers;

d) Maintaining Esko's Digital Information Security strategy;

e) Ensuring that Digital Information Security is part of the enterprise strategic planning process;

f) Reviewing and approving variances to Digital Information Security policies and standards;

g) Ensuring Esko adherence to Digital Information Security policies;

h) Ensuring Esko adherence to legal, regulatory and compliance requirements pertaining to Digital Information Security;

i) Reviewing Security Events and Security Incidents as necessary;

j) Monitoring changes in the exposure of information and Esko IT Assets to security threats; and

k) Implementing and overseeing a Continuous Improvement process to promote Esko's commitment to Continuous Improvement of its established Digital Information Security environment.

## 2 Acceptable Use Policy

The Acceptable Use Policy (AUP) defines appropriate uses of Esko Data and Esko IT Assets by users. Users shall keep confidential the use of internal information and security mechanisms and controls unless otherwise authorized to disclose certain information. Usage must be consistent with Esko values, mission, not illegal and not against Esko Code of Conduct. Esko provided assets are only meant to be used for business purposes. Incidental personal use of Esko IT assets is permitted, if it does not interfere with Esko's ability to perform its mission and meets the conditions outlined in Esko policies and guidelines.

a) Users shall maintain proprietary Esko data stored on any information storage or processing devices or systems in accordance with the AUP.

b) Immediately report any actual or possible theft or unauthorized use of passwords/passphrases, Esko Data, or assigned Esko IT Assets to Esko IT department in accordance with local Procedures.

c) Users may access, use, or share Esko Data only to the extent it is required, and are authorized to do so to fulfil assigned job duties as permitted by applicable local law or regulation.

d) Users must take reasonable precautions to ensure passwords/passphrases are protected against loss, theft, compromise, or misuse.

e) Users may only download or otherwise use appropriately licensed software authorized by Esko IT department on Esko IT Assets.

f) Users may use software purchased or approved by Esko only for its intended business purpose consistent with Esko IT department policies for software installation.

g) Users assigned a portable device Esko IT Asset must take it with them when leaving the office each night to facilitate business resiliency or telework.

h) Users must lock devices when unattended and never leave a device unattended in a public place.

i) Users are responsible for protecting against the loss, theft, or damage to Esko IT Assets assigned to their person including but not limited to computer systems, mobile devices and portable storage drives issued.

j) Users must take measures to prevent the spread of viruses, worms, phishing email messages, and malware by not installing unauthorized software, being careful when clicking on any links contained in e-mails, and not opening links or attachments from unexpected senders.

k) Users may only use Esko IT Assets to make statements on social media in accordance with the Esko Code of Conduct and Esko Social Media Guidelines.

l) Incidental personal use of Esko IT assets is permitted if it does not interfere with Esko's ability to perform its mission and meets the conditions outlined in Esko policies and guidelines.

    i. Esko is responsible for creating guidelines concerning personal use of computer systems, including Internet usage, consistent with any applicable collective bargaining agreement and where applicable, local law, regulation & Works Councils.

    ii. Users are responsible for following Esko guidelines and exercising good judgement regarding the reasonableness of personal use of Esko IT Assets.

    iii. In the absence of policy or uncertainty of usage, users should consult with their immediate manager/supervisor or Esko Human Resources Leader.

    iv. In all events, Esko reserves the right in its sole discretion to determine if personal use is excessive.

    v. Personal use of Esko IT Assets is subject to search and monitoring as described above consistent with any applicable collective bargaining agreement and applicable local law or regulation.

# 3 Risk Assessment and Management

a) Esko Digital Information Security is required to maintain a Digital Risk Register for identifying, assessing, and articulating security risks to facilitate decision making and prioritization of countermeasures.

b) Digital Risk Register is visible to the Esko CISO

c) Any Esko Digital Information Security Policy variances are recorded in the Esko Digital Risk Register.

d) Risk assessment procedures are performed when significant changes happen to Esko's operational, financial, reputational, or organizational risk level arising from third-party suppliers, contractual changes, audit findings, incidents, and technical or business initiatives.

e) The Digital Risk Register are reviewed and approved at a minimum annually by Esko leadership based on security risk rating according to the Risk Management Framework Standard.

f) Appropriate digital information security risk management and due diligence processes are performed for Esko merger and acquisition transactions and for Esko divestitures.

# 4 Non-Corporate-Owned Assets (Personal Devices)

## 4.1. Network Access

a) Non-corporate-owned assets are not permitted to connect to the corporate Esko network, except for any designated guest network.

b) Non-corporate-owned assets must not be used for Remote Access to the corporate Esko network unless they are subject to no less than the following controls:

i. Asset must not have any identified critical or high vulnerabilities

ii. Endpoint Detection and Response (EDR) must be present and enabled

iii. Asset must be up to date on current patching to within 30 calendar days.

iv. Asset must be subject to full disk encryption

v. If Asset runs iOS and/or Android, Esko approved mobile end-point security software must be installed and enabled.

c) Esko Security team may take unilateral action to remove a device from the network.

## 4.2. Data Access

a. Esko Data must not be stored on or transferred to or from any non-corporate-owned system or device without prior written approval from Esko Digital Information Security.

# 5 Data Privacy

a) Esko must adhere to the Global Privacy Policy and the Privacy Handbook.

## 6 Security Education and Awareness

a. Esko Digital Information Security coordinates a documented Digital Information Security Education and Awareness Training (SEAT) program for all users

b. Digital Information Security responsibilities, practices, and policies are communicated during onboarding orientation to new associates who use or access information systems no later than 90 calendar days after their start date.

c. Associates who use or access information systems must participate in security education and awareness training and exercises at least annually.

d. Esko is responsible for identifying which contingent workers are in scope for Esko Digital Information Security Education and Awareness Training (SEAT) based on their level of access to Esko IT Assets and/or Esko Data.

## 7 Security Event Management and Reporting

a. All users play a role in reporting suspected or actual digital information security events to Esko leadership in an expeditious and confidential manner.

b. Esko leadership is required to report potential digital information security incidents to the Esko Security team.

c. If the investigation reveals the data contains Personal Data, then the Data Protection Officer (DPO) must be notified immediately and will determine if the local Data Protection Authority (DPA) must be contacted.

d. Only Esko leadership may formally declare the occurrence of a digital information security incident.

e. A Esko Security Event Escalation Form must be submitted within 24 hours for investigation.

f. Esko leadership has a responsibility to support and fully comply with investigative procedures during a digital information security incident.

g. Esko Security team provides and maintains the Global Security Incident Response Plan to set forth the procedures, process, and governance structure for responding to and handling a Digital Information Security incident.

## 8 Data Protection and Recovery

### 8.1 Data Protection Program

- A Data Protection Program shall be established by Esko and incorporated at Esko for the appropriate classification, handling, processing, and protection of Esko Data.
- A Data Protection Officer (DPO) is appointed to handle all privacy related topics.
- The Data Protection Program includes a Data Classification Policy to serve as a framework for Esko to classify Esko Data according to the defined classification tiers for data protection enforcement.
- Data retention periods are formally documented and approved by Esko leadership to ensure they meet business, legal, regulatory and compliance requirements; data shall be retained according to the documented schedules set forth by Esko.

- When leaving their workspaces for the day, users must clear their desks and the surrounding area of non-public information and ensure papers and storage devices are protected according to their classification as described in the Data Classification Policy.

### 8.2 Backup & IT Disaster Recovery

- Esko maintains and adheres to documented backup standards to ensure the availability of Esko Data and Systems in line with business, legal, regulatory and compliance requirements.
- Backup and IT disaster recovery procedures shall facilitate business recovery procedures and restoration of business processes as defined by Esko.
- Esko ensures that testing and documentation of the results of backup and IT disaster recovery procedures are completed at least annually for Critical Technologies and at least every three years for non-critical technologies.

## 9 Identity and Access Management (IAM)

Esko implements safeguards and monitors usage of accounts and user identities used to gain access to Esko Assets and Data to prevent occurrences of unauthorized access.

### 9.1. Access Management

#### 9.1.1. Granting Access

a. Access credentials must uniquely identify an individual user, system, service, or application to prevent sharing of accounts. The access credentials must be adequately safeguarded.

b. Account access requests must be approved by authorized approver(s) for the job role or system.

c. Access requests must be auditable, and evidence of account approvals must be retained for a minimum of 12 months.

d. Accounts shall be granted with the bare minimum level of access necessary to perform specified job responsibilities.

#### 9.1.2. Granting Access

a. Esko associates play an important role in the timely removal of access. Voluntary and involuntary terminations must be entered into the HR system of record on or before the actual last day worked for the user, and the last day the account is required for non-user accounts.

b. Esko IT department shall initiate actions to remove access for terminated accounts immediately upon receiving notification up to a maximum of 2 business days after receiving the notification.

c. Accounts must be disabled after 90 calendar days of inactivity

d. Contingent worker and vendor accounts shall expire on the contract termination date or conclusion of work, whichever is earlier.

#### 9.1.3. Transferring Access

a. Job change transfers must be approved in the HR system of record prior to transfer date and prior to modifying access rights.

b. Access to Esko IT Assets and Esko Data must be reviewed based on the needs of the new role for applicability within 30 calendar days of transfer date.

#### 9.1.4. Shared, System Built-in and Service Accounts

The use of Shared and System Built-in accounts across multiple users in place of individual user accounts is prohibited, except for known and documented circumstances, and only with the prior review and approval by Esko IT / Esko Digital Information Security.

a. Shared, System Built-in and Service Account passwords/passphrases must be periodically changed in accordance with Esko password standards.

b. Each Shared, System Built-in or Service Account shall have the least level of privileges possible to perform its function.

c. Service Accounts shall be used by a single application or process function.

d. Shared, System Built-in, Service Accounts must have an assigned owner, process or software name, validated business justification and password/passphrase age that is stored in a secure central repository.

e. Shared, System Built-in and Service Accounts must follow Esko password policy requirements (Section 9.2.1) wherever technically feasible. Where not technically feasible, mitigating controls must be in place, subject to prior review and approval by Esko Digital Information Security.

#### 9.1.5. Access Reviews

a. Privileged Account access is reviewed on a quarterly basis and signed-off by an authorized approver.

b. Third-party accounts for contractors, vendors, or contingent workers are reviewed for termination or change of duties on a quarterly basis and signed-off on by an authorized approver.

c. Critical Technologies and/or applications is reviewed on a quarterly basis for separation of duties conflicts and level of access.

d. Shared, System Built-in and Service accounts are reviewed annually for applicability and have an identified owner.

## 9.2. Authentication Practices

Minimum authentication requirements must be met by Esko IT Assets and Esko Data, unless not technically feasible. Where not technically feasible, an Esko Digital Information Security Policy variance must be approved. This is applicable for computing systems that have network connectivity including individual and departmental accounts, applications, systems, and devices.

#### 9.2.1. Minimum Password/Passphrase Requirements

a. Passwords/passphrases and other authentication credentials must be secured and are considered confidential Esko Data.

b. Accounts must be set to meet minimum password/passphrase requirements, or credentials of at least equivalent strength, unless functionally restricted.

   i. Minimum password/passphrase requirements:

      ▪ Minimum length of 15 characters;
      ▪ Must contain 3 of the following attributes:
         - Upper case alphabetic;
         - Lower case alphabetic;

        - Numeric; and
        - Special character;
    - Users are prohibited from re-use of their previous 10 passwords;
    - Complexity requirements must be enforced;
    - Forced to change after initial authentication;
    - Incorrect credentials must result in an account being locked out:
        - After no more than 6 incorrect attempts; and
        - Until an administrator unlocks the account (higher security) or a predetermined period of time greater than or equal to 30 minutes (lower security); and

c. Passwords/passphrases must have a maximum age of 180 calendar days.

d. First time passwords/passphrases issued by IT must be unique and follow Esko password policy requirements (Section 9.2.1), and require changing upon first log in. First time passwords/ passphrases and other sign-in credentials such as username must be communicated via separate messages. It is recommended to use separate communication channels for usernames and first-time passwords/passphrases.

e. Password/passphrase manager or password/passphrase vault use is encouraged, as users will have multiple sets of credentials to perform their job functions. Refer to Esko IT departments for approved password management solutions.

f. Enterprise-class biometric systems may be used in addition to passwords/passphrases.

#### 9.2.2. Password/Passphrase Resets

a. User identity must be verified before a password/passphrase may be reset.

b. When a password/passphrase is reset or issued to new users, it shall be a unique value not known by individuals other than the administrator resetting the password/passphrase and the user, and the password/passphrase must be changed upon first login.

#### 9.2.3. Authentication Requirements

a. End user access to on-premises Critical Technologies, internet-facing IT systems and public cloud-based SaaS solutions shall be authenticated through Esko single sign-on (SSO) or another approved centralized identity and authentication repository where technically feasible.

b. The use of Multi-Factor Authentication (MFA) is required to gain access to Internet-facing IT systems and public cloud- based SaaS Solutions.

c. Authentication processes must utilize encryption while in transit. Passwords/passphrases must be encrypted at rest in storage or use similar protection methods.

### 9.3. Administrator Account Management

#### 9.3.1. Administrator and Privileged Access

a. Administrative rights and access to a desktop, laptop, and/or other Esko IT Asset is a privilege only provided to authorized Esko users with validated business justification for the access.

b. Users with administrator access are required to maintain separate accounts, one with standard user access and one with administrator access. The usernames and passwords/passphrases for the two separate accounts are to be unique to each account and have no replication between them.

c. Procedures shall be established such that any shared administrator account passwords/passphrases are reset when any user with access to the administrator password/passphrase separates from the organization or changes roles such that access to the shared account is no longer required for job duties.

d. Administrator passwords/passphrases follow password policy requirements (Section 9.2.1)

e. Administrator access to enterprise systems must require Multi-Factor Authentication (MFA).

#### 9.3.2. Segregation of Duties

a. Requests for new hires and access changes must take consideration of the possible segregation of duties conflicts the access changes will reflect. It is the responsibility of both Esko leadership and the administrators to ensure proper segregation and prevent excessive access to any systems.

b. Appropriate due diligence must be performed by the information or process owner, to ensure access granted to an individual does not create a segregation of duties conflict.

# 10 Third Party Management

## 10.1 Due Diligence and Risk Assessment

a. Due diligence, including but not limited to investigation into Esko history/performance and risk assessment, must be performed prior to sharing confidential or restricted data with third party service providers or allowing them to access Esko IT Assets or provide mission critical services.

b. Esko business sponsors and IT/Security teams along with legal, finance and procurement must formally approve third-party service provider risk assessments prior to contract signing or payment. Esko Security tem will conduct security risk assessments for organization-wide services.

c. Cloud Service Providers must have a formalized security program and ideally have a third-party accredited firm perform an annual attestation on their internal controls and generate a report to be shared (like a valid SOC 2 Type II report).

d. Cloud Service Providers must adhere to Esko third party due diligence, risk assessment, compliance, contractual, and monitoring requirements.

## 10.2 Responsibilities and Contractual Agreements

a. Third party service providers must formally accept responsibility for the digital information security of maintained data, continued compliance with business, legal, regulatory, compliance or industry requirements, and adherence to established service level agreements (SLAs) in executed contracts.

b. Cloud Service Providers must fully cooperate with any legal investigations (including e-discovery) in a timely manner, required as a part of a digital information security incident or data breach.

## 10.3 Monitoring Program

a. Esko leadership must verify that critical third party service providers maintain an effective digital information security program at a minimum annually.

## 11 Cloud Security Protections and Considerations

To ensure the integrity of data, contracts with cloud service providers must address the following, at a minimum:

a. Services obtained by a Cloud Services Provider must adhere to Esko procurement program. Users must not use cloud services in a manner that circumvents security, procurement, legal and finance approval and sign-off process including but not limited to using a credit card for payment.

b. Cloud Service Providers are prohibited from mining Esko Data at any time without express prior written authorization of Esko.

c. If Cloud Service Providers store or have access to sensitive Esko Data, Esko's standard privacy language for vendor contracts is included.

d. Cross-border data transfers will require the appropriate regulatory and legal filing.

e. Esko maintains all ownership rights to data hosted by Cloud Service Providers, even while residing within the environment of a Cloud Service Provider.

f. Cloud subscriptions must be affiliated to an Esko issued account and tied to an Esko approved identity system of record.

g. Esko cloud-based systems should adhere to Esko cloud standards.

## 12 Physical and Environmental Security

### 12.1 General Physical Access

a. Physical access to facilities must be controlled via electronic badge access systems, with everyone requiring access obtaining an individually assigned access badge.

b. Facilities access will be restricted to individuals based on organization requirements and job function.

c. Entry and exits to restricted areas must be monitored and recorded 24/7/365 by digital means and stored for a period of at least 180 calendar days unless otherwise prohibited by local law or regulations. Esko must comply with applicable local law or regulatory requirements regarding notifying users and others of any such monitoring.

d. Visitors, contractors, and vendors are required to display badges, and must sign in and out with recorded details of the visit (e.g., name, date, time in, time out, firm represented, associate escort). Visitors must be escorted by an Esko associate at all times.

### 12.2 Remote working and Teleworking

Remote working and Teleworking are permitted as long as Esko provides approval prior to the start of remote work or telework. Alignment with Esko HR is essential.

### 12.3 Data Center Access

a. Physical access to a data center, data room, and supporting utilities must always be locked and restricted to those individuals requiring access based on job duties.

b. Esko is required to semi-annually validate the authorized entry list and ensure only authorized individuals access the data center.

c. When access to workstations, servers or other consoles in the data center is not needed, they must be locked out or the user must log out of the system.

d. A visitor log for the data center must be maintained and stored for a period of at least 180 calendar days. Visitors must be escorted in the data center by an Esko associate at all times.

### 12.4 Environmental Protections

a. Temperature, humidity, water, and fire controls must be implemented and maintained to ensure proper functioning of the equipment housed in the data center.

b. Monitoring and alerting mechanisms must be implemented to notify facilities and/or systems administration associates when less than optimal environmental conditions are reached in the data center.

## 13 Asset Management

a. Esko maintainq an accurate inventory of Esko IT Assets identifiable by a unique asset name, business user, IT owner, data sensitivity level, and business criticality.

b. The inventory of IT assets is stored in a central secured repository, electronically searchable, reviewed, and updated on a regular basis.

c. The scope of Esko IT asset management programs shall, at a minimum, include:

   i. Critical Enterprise Technologies and supporting software, databases, and infrastructure

   ii. Databases and data repositories containing Restricted data

   iii. Esko IT Assets including: Esko owned and managed workstations, laptops, iOS and Android devices (e.g., phones and tablets

   iv. Network devices (e.g., routers, switches and firewalls)

   v. External IP addresses and address ranges; Internal IP address ranges

   vi. External DNS domains

   vii. Cloud environments (e.g., subscription Accounts, availability zones, VPCs, and related records as appropriate for the specific cloud platform)

d. All associates and contingent workers must return Esko issued assets upon termination of employment or contract.

e. Esko must securely dispose of Esko IT Assets according to the Data Sanitization Standard when decommissioning or repurposing the asset.

## 14 Change and Configuration Management

a. Esko had a formalized and documented configuration management process whereby changes are formally documented, approved, and communicated.

b. Esko has a formalized and documented change management process whereby changes are formally documented, approved, and communicated.

c. Formal approval, testing documentation, and communication of changes to the Production environment is retained and auditable for 12 months.

d. Emergency changes are permitted only under the condition that formal documentation, approval, and communication is performed timely and completely.

## 15 Product Security

Esko follows the Global Product Security Policy and the Product Security Framework.

## 16 Secure Enterprise Software Development

a. Esko maintains a documented Software Development Life Cycle (SDLC) that includes security gates/practices that ensure security by design.
b. Access to application production environments is restricted to users who require access due to assigned job duties.
c. Application source code is stored and tracked in code versioning repositories with access restricted to users who require access based on assigned job responsibilities.
d. Code reviews, whether manual by a peer or using scanning tools, are performed on developed applications prior to release into the production environment. A developed application cannot be released into the production environment in any case where code reviews reveal critical or high security vulnerabilities.
e. Associates developing software or software scripts and those responsible for code review shall participate in an annual secure coding training to understand and identify common code security risks.
f. Summary results of code reviews can be shared with external customers after approval from the Esko CISO under NDA.
g. API keys and similar secrets must be securely stored in central repositories.
h. The use of Multi-Factor Authentication (MFA) is required to gain access to production environments.
i. Esko is responsible for defining and maintaining open-source use and review policies for developed applications.
j. Esko has a duty to maintain developed applications for as long as they remain accessible on the production environment

## 17 Network Security

Esko implements safeguards and monitors usage of the Esko Network to protect Esko IT Assets and Esko Data. Esko follows the Network Security Standard.

## 18 System Security

a. Esko IT Assets minimum security configuration baseline standards is documented, established, and maintained by Esko for each system type, whether hosted on premises or with a cloud service provider.
b. Esko IT Assets are required to meet the established, documented minimum security

requirements before accessing production resources and networks.

c. Full disk encryption are configured and activated on Portable IT Assets.
d. Access to removal media are restricted based on business justification.
e. Esko issued Mobile Devices have the ability to be remotely wiped (e.g., smart phones, tablets).
f. Esko Digital Information Security approved Endpoint Detection and Response (EDR), Vulnerability Management (VM) and logging solutions are implemented and maintained on Esko IT Assets.
g. When known insecure or not generally available (Beta) version of software is required to be installed on the network, the architecture including any mitigating controls must be approved by the Esko CISO and the Threat Management Center (TMC) must be notified via security@esko.com
h. Esko IT systems and Mobile Devices are password/passphrase protected with an active automatic screen lock feature that activates after 15 minutes or less of inactivity.
i. Esko is responsible for maintaining information system logs and audit trails according to the Esko logging standards that may be used for forensic investigation purposes.
    i. Audit trails are readable, exportable, and able to be presented to Esko Digital Information Security if requested during a security incident response.
    ii. Audit trails must be protected to prevent unauthorized access and to maintain integrity from tampering.

## 19 Security Monitoring and Logging

a. Esko configures information systems to log significant IT system security events to aid in security investigations and to meet business, legal, regulatory and compliance requirements as defined in Veralto Logging Standard.
b. Required logs from on-premises and Cloud are stored in a centralized logging repository and made available for security analysis.
c. Required logs are analyzed for cyber threat activity by the Threat Management Center (TMC)
d. System owner shall ensure log data is retained in accordance with legal record retention requirements, as well as other applicable legal, regulatory, and compliance requirements.

## 20 Vulnerability Identification and Management

### 20.1 Vulnerability Management

a. Esko complies with the Vulnerability Management Standard to ensure the timely identification, remediation, and reporting of digital information security vulnerabilities.

b. Esko has a Coordinated Vulnerability Disclosure (CVD) program for ethical hackers https://www.esko.com/en/legal/coordinated-vulnerability-disclosure

### 20.2 Penetration Testing

a. Esko complies with the Vulnerability Management Standard and the Penetration Testing Guidance.
b. Esko notifies Esko Security team via security@esko.com prior to conducting penetration testing on any internally routable environment.

c. The results of the penetration testing are disclosed to the Esko Security team and Esko leadership.

d. Third-party penetration testing service providers must go through third-party risk assessment prior to engagement.

## 21 Security Assessments and Audits

- Esko provides available relevant external security audit reports upon request.
- Esko allows security assessments or audits performed by customers or their authorized professional representative and provides all assistance reasonably required, provided that the customer respects the Esko Audit Request Process (including at least three weeks advance notice).
- Esko allows a security assessment or audit once per calendar year.
- Esko is not responsible for any costs associated with a security assessment or audit as performed by customers or their authorized professional representative.
- Esko shall remedy any identified security deficiencies which are confirmed and acknowledged and this in a timely manner in alignment with Esko planning.

****** END OF DOCUMENT ******