INFORMATION SECURITY (IS) POLICY

Version	1.0
Status	Final
Classification	Public

DOCUMENT SIGN OFF

Document Version : 1.0	
Author **Name : Michael Alexander Djojo** **Position : IT Infrastructure** **Date : 18 November 2024**	
Reviewer & Approver **Name : Budhi Tjahyono** **Position : IT Business Unit Head** **Date : 18 November 2024**	

VERSION CONTROL

Version	Date of publish	Author	Summary of change
1.0	18 November 2024	Michael Alexander Djojo	Initial document

TABLE OF CONTENT

1. BACKGROUND AND PURPOSE

Information security controls are an essential aspect within an organization's ISMS. They are designed and implemented to control any relevant information security risk that was previously identified.

The information security controls are designed and implemented to reduce the likelihood and/or reduce the impact of information security risk. The design and implementation of the controls were done by considering the preservation of the confidentiality, integrity, and availability of the organization's information.

This policy serves as a guideline for the information security controls implemented in PT Dynaplast ("Dynaplast").

2. SCOPE

This policy applies for all personnel, information, information processing facilities and its supporting utilities within the scope of the ISMS in Dynaplast.

3. RESPONSIBILITY

1. The ISMS's Management representative is responsible for the overall implementation of the processes and activities described in this policy.
2. The ISMS top management is accountable for the overall implementation of the processes and activities described in this policy.
3. The ISMS Governance and Secure Development is responsible for the review and maintenance of this policy.

4. REFERENCE

- All Annex ISO 27001:2022.
- Dynaplast Information Security Management System (ISMS) Manual

5. INFORMATION SECURITY GOVERNANCE

5.1. General Management

Dynaplast's information security policy provides management direction, support, and guidelines for implementing the organization's Information Security Management System (ISMS) and controls. This policy aligns with business requirements and relevant laws and regulations, ensuring it is approved, published, and communicated to employees and external parties. The policy is reviewed annually or after significant changes to ensure its relevance, with any modifications being documented and controlled.

Dynaplast also defines clear information security roles and responsibilities, including segregation of duties to mitigate risks of fraud or errors. The organization maintains documented operating procedures for information processing and communication facilities, ensuring they are accessible to relevant employees. Additionally, Dynaplast specifies contacts for legal, regulatory, and industry-related matters, ensuring compliance and alignment with security forums and professional associations.

5.2. Management Engagement

Employees at Dynaplast are briefed by management on their information security roles and responsibilities and are provided guidelines to protect the organization's assets. They are expected to comply with all relevant laws, policies, and procedures, and the organization ensures they possess adequate information security skills and qualifications. Additionally, a confidential channel is available for reporting violations of the information security policy.

5.3. Compliance With Legal and Contractual Requirements

Dynaplast ensures compliance with all legislative, regulatory, and contractual requirements by explicitly identifying, documenting, and updating them for all information systems. The organization adheres to intellectual property laws, inventories, and manages software licenses, and safeguards important records against loss, falsification, or misuse. Dynaplast also ensures the privacy and protection of personally identifiable information and applies cryptographic controls in accordance with relevant laws, regulations, and agreements.

5.4. Clear Desk and Clear Screen

Sensitive documents, critical business information, and removable storage media shall be securely locked away when not in use, and user devices shall be locked or logged off when unattended. Devices shall be configured with timeout or auto-logout features, unnecessary pop-ups disabled during public use, and sensitive information cleared from displays and whiteboards after use. Printed materials shall be collected immediately, and sensitive documents and media securely disposed of when no longer needed. For detailed procedures, refer to the Acceptable Use of Assets Guideline.

6. INFORMATION SECURITY RISK

The risk management process is conducted to balance information security risks with the operational and business requirements of the organization. This is done using an iterative process that includes the risk assessment, risk treatment, risk acceptance and risk communication activities.

All organization risk management processes need to be done at least annually or when relevant and significant changes are proposed or occur in the organization. Records related to the risk management process shall be established and maintained.

7. ASSET MANAGEMENT

Dynaplast ensures all assets related to its information and processing facilities, including information, software, hardware, and supporting facilities, are identified, inventoried, and assigned to the IT Department as the asset owner. The IT Department is responsible for managing and securing these assets, ensuring they are inventoried, classified, and handled per Dynaplast's information classification and handling policy.

Employees, contractors, and third parties shall adhere to Dynaplast's acceptable use policies, including guidelines for email, internet usage, and mobile devices, particularly when used outside the organization's premises. Assets shall be returned upon the end of an individual's employment with Dynaplast, such as in cases of resignation or retirement.

8. ACCESS MANAGEMENT

Dynaplast ensures secure device reuse by implementing secure formatting, reinstalling operating systems, and removing residual data. User access management follows formal processes, including registration, de-registration, and disabling invalid or redundant User IDs, while enforcing segregation of duties and access authorization in line with legal and contractual obligations. Access to program source code and libraries is managed based on business needs to prevent unauthorized alterations.

Each identity is assigned to a single person to ensure accountability, with exceptions for shared identities requiring documented approval. Identities no longer needed are reviewed and removed within three months of termination while maintaining audit trails. Logs of identities and authentication information are maintained for oversight.

Dynaplast shall implement authentication processes, with temporary and unique authentication information, such as passwords or PINs, generated automatically. Users shall secure their authentication credentials, including passwords, pins, access cards, and tokens.

Access rights are granted based on business needs, adhering to the principle of minimum privilege. Rights are regularly reviewed and updated as roles or responsibilities change. Privileged access is

strictly limited to authorized personnel, revoked upon employment changes, and assigned individually wherever possible to ensure accountability and prevent sharing.

9. THIRD PARTY SECURITY MANAGEMENT

Dynaplast identifies and documents all IT third-party service providers, including details of the services provided and associated contracts. Supplier selection considers competence, experience, service delivery capability, and resilience during disruptions. Contracts with suppliers shall include confidentiality agreements, adherence to Dynaplast's information security requirements, defined responsibilities, and assurances that subcontractors shall also comply with these standards. Supplier access to Dynaplast information and assets is granted on a need-to-know basis with formal approval, and supplier personnel shall be informed of and adhere to Dynaplast's security requirements, including signing confidentiality agreements.

Dynaplast establishes formal agreements with suppliers covering IT infrastructure security, data protection, access controls, incident response processes, regulatory compliance, and Dynaplast’s right to audit or monitor compliance. Contracts include provisions for service-level obligations, incident communication protocols, and regular performance reviews or audits to verify compliance. When supplier relationships are terminated, Dynaplast ensures the revocation of access, the return or secure deletion of Dynaplast assets and sensitive data, and the prevention of unauthorized post-termination access.

10. CLOUD SECURITY

All cloud services must comply with Dynaplast’s information security requirements for confidentiality, integrity, and availability, with their usage scope documented and management roles assigned to the IT department. Cloud service agreements should align with security standards, include SLAs for confidentiality and availability, and ensure access control, malware protection, and secure data handling. Providers must notify Dynaplast of significant changes, such as data relocation or subcontracting, and seek approval for such actions. Security incidents must be promptly reported, with providers offering resolution support. Cloud services should include backup and recovery mechanisms, ensure secure data return or deletion upon termination, and maintain clear communication channels for addressing service-level issues and security concerns.

11. INFORMATION SECURITY INCIDENT MANAGEMENT

Incident management at Dynaplast is overseen by the IT department, with a structured reporting process involving the IT Support, IT Infrastructure Support, and IT Infrastructure Operation teams. Reporting utilizes the IT ticketing system to guide necessary actions, while documented procedures ensure swift and effective responses through detection, prioritization, analysis, communication, and coordination, as detailed in the Information Security Incident Management Procedure. Security incidents are analyzed to determine appropriate handling, including identifying and classifying the incident, assessing its impact and root cause, and making decisions on response strategies, escalation, and communication plans. Lessons learned are integrated into future processes to enhance incident management.

12. BUSINESS CONTINUITY PLAN (BCP) & DISASTER RECOVERY PLAN (DRP)

Dynaplast integrates information security continuity requirements with corporate business continuity plans to safeguard operations during and after disruptions or disasters. This includes defining techniques, methods, and infrastructure necessary for maintaining information security, supported by documented processes, procedures, and controls to ensure resilience in challenging circumstances.

The Disaster Recovery Plan encompasses procedures for activating and recovering redundant components and processing facilities, aligned with business continuity objectives and ICT requirements identified through a Business Impact Analysis (BIA). Regular testing, including

scheduled and ad-hoc drills, ensures the effectiveness of backup, failover, and restoration processes, strengthening Dynaplast's ability to recover from disruptions.

13. IS LEGAL, DATA PRIVACY, and PROTECTION COMPLIANCE

Dynaplast shall ensure compliance with all relevant legislative, statutory, regulatory, and contractual requirements for each information system and across the organization. This includes maintaining up-to-date documentation on how Dynaplast meets these requirements, managing proprietary software in compliance with intellectual property laws, and protecting important records from loss, misuse, or destruction. Privacy and protection of personally identifiable information, along with the use of cryptographic controls, shall also be in line with relevant laws and regulations.

Dynaplast is committed to intellectual property rights compliance, acquiring software only from reputable sources. Intellectual property requiring protection shall be identified, and asset registers shall be maintained to ensure accountability. Proof of ownership for licenses and materials shall be kept demonstrating compliance, and Dynaplast shall regularly review software and information product usage to ensure only authorized, licensed assets are used. Secure disposal or transfer procedures shall be in place to comply with applicable licenses and agreements.

A retention schedule for records shall be defined, detailing the types of records and their retention duration. Records shall be securely stored according to this schedule and can be retrieved within an acceptable time frame and format, as required by applicable regulations.

Dynaplast's approach to information security shall be reviewed annually by the Internal Audit team or when significant changes occur. Managers shall regularly review compliance within their areas of responsibility, ensuring that information processing and procedures align with security policies and standards. Additionally, regular reviews shall be conducted to ensure Dynaplast's information systems comply with relevant security standards.

14. HUMAN RESOURCE SECURITY

Dynaplast performs background verification checks for all employees, customers, and third-party candidates in line with relevant regulations. These checks may include verifying character references, CV details, academic and professional qualifications, and criminal records. The screening process is documented, and all employees, contractors, and third parties must sign employment contracts acknowledging their responsibility for securing Dynaplast's information.

During employment, all employees, contractors, and third-party personnel must follow Dynaplast's security policies and procedures. Regular training and socialization on information system security are mandatory for employees based on their roles and responsibilities. Customers and third parties may also undergo security awareness training, and employees who violate information security policies shall face disciplinary actions in line with Dynaplast's policies.

Upon termination or a change in employment, Dynaplast defines and enforces ongoing information security responsibilities, as specified in contracts and confidentiality agreements. All assets must be returned, and access rights shall be disabled or adjusted accordingly, ensuring proper management of security responsibilities after employment changes.

15. PHYSICAL SECURITY

Dynaplast premises must be secured from unauthorized physical access and environmental threats. Essential equipment and utilities that support Dynaplast service delivery should be properly secured, regularly maintained, and tested. The premises shall have a secure physical perimeter to prevent unauthorized access, with entry points manned by security personnel. Access is controlled and monitored, and areas are classified into public, limited, and restricted, with appropriate access controls for each. Security-sensitive activities and restricted areas shall be monitored, and the use of photographic or video recording devices is restricted.

Within Dynaplast premises, all personnel and visitors must wear identification tags, and visitors to restricted areas must request formal permission and be supervised. Delivery areas are secured and monitored, and materials are inspected before moving. Additionally, Dynaplast's premises shall be protected against natural and man-made disasters, such as fire, flood, and earthquakes.

Dynaplast equipment, especially within control rooms, must be kept in secure environments, continually monitored, and regularly maintained according to the manufacturer's recommendations. Activities like eating, drinking, and smoking are prohibited in these areas. All power and telecommunications cables must be protected from damage or interference. Equipment must not be removed from the premises without authorization, and disposal must be conducted securely to avoid any adverse impact on the organization or the environment.

16. DATA SECURITY

Dynaplast enforces compliance with privacy and protection procedures for personally identifiable information (PII), ensuring appropriate measures are in place to protect personal data from unauthorized access, processing, or disclosure. Clear roles and responsibilities are defined to ensure compliance with relevant legislation and regulations.

Information at Dynaplast is classified based on its sensitivity and the potential impact of a security breach. Formal guidelines are established to classify, label, and handle information appropriately, ensuring that all information is treated according to its classification. Additionally, all information, regardless of format, must be labeled according to the established classification scheme.

Dynaplast employs various methods for transferring information, such as electronic, physical, and verbal transfers, with appropriate controls in place to ensure the security of information during transit. Sensitive information is not retained longer than necessary, and secure deletion methods, including the use of certified providers, are applied when information is no longer needed. Data protection measures, such as data masking, pseudonymization, and anonymization, are employed for sensitive data, while data leakage prevention techniques are implemented to minimize risks. Backup copies of critical information are securely maintained according to Dynaplast's Backup Restore Procedure to ensure data availability.

17. INFORMATION SECURITY OPERATION (TECHNICAL CONTROLS)

Dynaplast ensures that systems and resources are optimized and monitored to meet business needs, with controls in place to prevent, detect, and respond threats/events. Secure configurations are maintained, and key activities are logged and monitored to address security incidents. Access to privileged programs is restricted and logged, while only approved software is installed following change management processes. Responsibilities for cloud services are clearly defined, and all systems use synchronized time sources. For further details on capacity management, malware protection, configuration management, logging, monitoring, privileged programs, software installation, cloud services, and threat intelligence, refer to the related policy.

18. NETWORK SECURITY

Dynaplast has implemented network segregation to ensure proper control and handling based on varying security requirements. For critical information systems, security gateways shall filter traffic, and network services such as internet, third-party, and wireless access shall be controlled to prevent unauthorized access. Access to diagnostic and configuration ports on Dynaplast's network and security devices, such as console ports, shall be restricted to Dynaplast's network administrators, approved third parties, and authorized monitoring applications.

19. SECURE SOFTWARE DEVELOPMENT LIFECYCLE MANAGEMENT (SDLC)

Dynaplast shall ensure separation between development and production systems, operating them in different domains. Sensitive information shall not be copied into development and testing environments unless specific exception controls are in place.

During the software development life cycle (SDLC), Dynaplast shall ensure the integration of security controls to protect information and systems against identified threats. Security controls shall be analyzed for their ability to prevent, detect, or respond to security events, with a focus on encryption, integrity checking, and digital signing. Secure coding principles shall be applied during all phases of software development.

Security risks shall be assessed early and continuously addressed throughout the project life cycle, with regular reviews and testing of the effectiveness of risk treatments. New systems and upgrades shall undergo thorough security testing against functional and non-functional requirements.

Dynaplast shall manage access to program source code and ensure proper configuration management, including disabling unnecessary functions, restricting powerful programs, and synchronizing clocks. Employees involved in application development shall complete application security training upon hiring and annually thereafter. All software and applications shall be licensed in accordance with vendor agreements and applicable laws, with alternatives such as open-source or free software available where applicable.

20. VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

Dynaplast shall maintain an accurate inventory of software assets, including vendor, software name, version, deployment status, and responsible personnel, to support effective technical vulnerability management. Roles and responsibilities for vulnerability management shall be defined, including vulnerability monitoring, risk assessment, asset tracking, and coordination efforts. Procedures shall be established to detect vulnerabilities in products, services, and external components.

All new information systems, upgrades, and versions shall undergo thorough testing and verification, with security testing conducted against defined requirements. This includes testing for security functions like user authentication, access control, cryptographic usage, secure coding practices, and the secure configuration of systems like operating systems and firewalls.

Audit activities involving Dynaplast’s information systems shall be carefully planned and managed to minimize disruptions to business operations. These audits shall verify the security and integrity of the information systems and ensure that any vulnerabilities are appropriately addressed.