Information Security Policy

(POL-01)

	Function	Name	Sign/Date
Prepared by			
Reviewed by			
Approved By			

Distribution List

Department Name	Copy No.	Checkbox
		☐
		☐
		☐
		☐
		☐
		☐
		☐
		☐

Document History

Issue No.	Issue Date	Changed Occurred/ Page Number	Res. Person

1. Purpose:

The purpose of this Information Security Policy is to establish the principles, requirements, and management direction for protecting the information and associated assets of **Asbab Technical Company**.

The objectives of this policy are to:

1.1 Protect the confidentiality, integrity, and availability of the Company's information and associated assets.

1.2 Establish a consistent and risk-based approach to managing information security.

1.3 Align information security objectives with the Company's strategic and operational objectives.

1.4 Define information security responsibilities and accountability across the Company.

1.5 Ensure that information security risks are identified, assessed, treated, monitored, and periodically reviewed.

1.6 Provide a framework for implementing, maintaining, monitoring, and continually improving information security controls.

1.7 Protect information belonging to the Company and, where applicable, information entrusted to the Company by customers, suppliers, employees, or other interested parties.

1.8 Ensure compliance with applicable legal, regulatory, statutory, contractual, and organizational requirements.

1.9 Protect information throughout its lifecycle, including its creation, processing, storage, transmission, sharing, retention, and secure disposal.

2. Scope:

2.1 This policy applies to all information, information assets, systems, processes, facilities, technology resources, and services owned, operated, managed, or used by Asbab Technical Company, as applicable.

2.2 This policy applies to all employees, management, contractors, consultants, temporary personnel, suppliers, service providers, and other third parties who access or handle the Company's information or associated assets.

2.3 The policy applies to information in all forms, including electronic, digital, physical, verbal, and recorded information.

2.4 Where the Company processes or handles information on behalf of customers or other parties, such information shall be protected in accordance with applicable contractual, legal, regulatory, and security requirements.

2.5 All users and relevant third parties shall comply with this policy and applicable supporting information security requirements.

3. Information Security Principles:

Asbab Technical Company shall manage information security based on the following principles::

3.1 Confidentiality:

Information shall be accessible only to authorized individuals, systems, or entities based on legitimate business requirements.

3.2 Integrity:

Information shall be protected against unauthorized or accidental modification, destruction, or corruption and shall remain accurate, complete, and reliable.

3.3 Availability:

Information and information processing facilities shall be available to authorized users when required to support business and operational activities.

3.4 Risk-Based Approach:

Information security controls shall be selected and implemented based on identified risks, business requirements, applicable obligations, and the Authority's risk acceptance criteria.

3.5 Least Privilege and Need-to-Know:

Access to information and systems shall be limited to the minimum level required to perform authorized responsibilities.

3.6 Security by Design:

Information security shall be considered during the acquisition, design, development, implementation, modification, and retirement of systems and services.

3.7 Continual Improvement

The effectiveness of the information security management system and its controls shall be continually evaluated and improved.

4. Management Commitment and Information Security Objectives:

4.1 Top Management shall demonstrate commitment to information security by providing appropriate direction, authority, resources, and support.

4.2 Asbab Technical Company shall establish, implement, maintain, and continually improve an Information Security Management System appropriate to its context, objectives, risks, and business requirements.

4.3 Information security objectives shall be established, monitored, reviewed, and aligned with the Company's strategic objectives.

4.4 Information security shall be integrated into relevant business processes and organizational decision-making.

4.5 Management shall ensure that significant information security risks and issues are appropriately addressed and escalated.

4.6 Information security policies and supporting documented information shall be maintained, controlled, communicated, and periodically reviewed.

5. Information Security Risk Management

5.1 Information security risks shall be identified, assessed, treated, monitored, and reviewed using an approved risk management methodology.

5.2 Risk assessments shall consider relevant threats, vulnerabilities, likelihood, potential impact, existing controls, and business consequences.

5.3 Security controls shall be selected based on the results of risk assessments and applicable legal, regulatory, contractual, and business requirements.

5.4 Information security risks shall be reviewed periodically and whenever significant changes occur to the Company's activities, systems, technologies, suppliers, threats, or regulatory environment.

5.5 Risk treatment decisions and accepted residual risks shall be documented and approved by authorized personnel.

6. Information and Asset Management:

6.1 Information and associated assets shall be identified, inventoried, assigned appropriate ownership, classified where required, and managed throughout their lifecycle.

6.2 Information assets may include, where applicable, information, records, hardware, software, systems, applications, devices, storage media, documentation, and other resources supporting the Company's activities.

6.3 Asset owners shall define appropriate protection requirements and ensure that assets under their responsibility are adequately protected.

6.4 Information and associated assets shall be used only for authorized purposes.

6.5 Assets and access rights shall be returned, removed, or appropriately managed when personnel or third-party relationships end or responsibilities change.

6.6 Information, equipment, and storage media shall be securely disposed of or reused in accordance with their classification, sensitivity, and applicable requirements.

7. Information Classification and Handling:

7.1 Information shall be classified according to its sensitivity, business value, legal and regulatory requirements, contractual obligations, and the potential impact of unauthorized disclosure, alteration, loss, or destruction.

7.2 Information shall be handled, stored, transmitted, shared, retained, and disposed of according to its classification and applicable security requirements.

7.3 Confidential and sensitive information shall be protected against unauthorized access, disclosure, copying, modification, transmission, loss, or disposal.

7.4 Information shall only be transferred through approved and appropriately protected channels.

7.5 Where information belonging to customers or other interested parties is handled by the Company, it shall be protected in accordance with applicable contractual and security requirements.

8. Identity and Access Management:

8.1 Access to information, systems, applications, networks, facilities, and other associated assets shall be authorized based on business need, least privilege, and need-to-know principles, where applicable.

8.2 Unique identities shall be assigned to users, where technically feasible, to ensure accountability and traceability.

8.3 User accounts and access rights shall be managed throughout their lifecycle, including creation, modification, periodic review, suspension, and removal.

8.4 Access rights shall be promptly reviewed and adjusted when users change roles, responsibilities, or employment or contractual status.

8.5 Privileged and administrative access shall be strictly controlled, authorized, and monitored based on risk.

8.6 Appropriate authentication mechanisms shall be implemented according to the sensitivity and risk associated with the systems and information.

8.7 Shared accounts shall be avoided and shall only be permitted where technically necessary and formally authorized.

8.8 Authentication information, passwords, keys, tokens, and other credentials shall be protected against unauthorized disclosure or use.

8.9 Remote access to organizational systems and resources, where provided, shall be authorized and protected through appropriate security controls.

9. Acceptable Use:

9.1 All users shall use information and associated organizational assets responsibly, securely, and only for authorized purposes.

9.2 Users shall comply with applicable information security policies, legal requirements, contractual obligations, and security instructions.

9.3 Unauthorized access, misuse, disclosure, alteration, destruction, or transfer of information is prohibited.

9.4 Installation or use of unauthorized software, applications, devices, storage services, or communication channels is prohibited where not explicitly authorized.

9.5 Users shall not disclose or share passwords, authentication credentials, security keys, or other authentication information.

9.6 Organizational information and associated assets shall not be used for unlawful, malicious, fraudulent, or unauthorized activities.

9.7 Users shall immediately report actual or suspected loss, misuse, unauthorized access, disclosure, or compromise of information or associated assets.

10. Human Resource Security and Awareness:

10.1 Information security responsibilities shall be communicated to employees and relevant third parties as part of their employment or contractual relationship.

10.2 Personnel shall receive appropriate information security awareness and training upon joining the Company and periodically thereafter.

10.3 Role-specific security training shall be provided where required based on responsibilities and identified risks.

10.4 Personnel shall protect confidential and sensitive information during and after their employment or contractual relationship.

10.5 Appropriate confidentiality and information security obligations shall be included in employment and contractual arrangements where applicable.

10.6 Security responsibilities and access rights shall be reviewed when personnel are transferred, change responsibilities, or leave the Company.

10.7 Violations of information security requirements may result in appropriate disciplinary or contractual action.

11. Physical and Environmental Security

11.1 Physical access to areas containing sensitive information or information processing resources shall be restricted to authorized personnel.

11.2 Appropriate physical security measures shall be implemented based on risk, including access controls, locks, surveillance, monitoring, and visitor controls where applicable.

11.3 Information processing facilities and equipment shall be protected against relevant physical and environmental threats.

11.4 Equipment, storage media, and physical information shall be protected against unauthorized access, theft, loss, damage, or misuse.

12. Technical Security:

12.1 Appropriate technical security controls shall be implemented and maintained to protect information and information processing resources against unauthorized access, misuse, loss, alteration, disruption, and malicious activities.

12.2 Protection mechanisms against malware and other technical threats shall be implemented where appropriate.

12.3 Security updates and patches shall be managed according to risk, system criticality, and applicable requirements.

12.4 Technical vulnerabilities shall be identified, assessed, prioritized, and addressed within appropriate timeframes based on risk.

12.5 Appropriate technical security measures, such as network protection, endpoint protection, access controls, monitoring, and security event detection, shall be implemented where required by risk.

12.6 Cryptographic controls and encryption shall be used where necessary to protect sensitive information based on risk and applicable requirements.

12.7 Security logs and events shall be generated, protected, monitored, and reviewed where necessary to support accountability, detection, and investigation.

13. Backup and Information Security During Disruption:

13.1 Critical information and information processing resources shall be backed up according to business, operational, and information security requirements, where applicable.

13.2 Backup copies shall be protected against unauthorized access, alteration, destruction, and other relevant threats.

13.3 Backup restoration and recovery capabilities shall be periodically tested where required to verify that critical information and resources can be recovered when needed.

13.4 Information security requirements shall be integrated into business continuity, disaster recovery, and crisis management arrangements, where applicable.

13.5 During disruptions and recovery activities, appropriate measures shall be maintained to protect the confidentiality, integrity, and availability of critical information.

14. Information Security Incident Management:

14.1 Asbab Technical Company shall maintain processes for identifying, reporting, assessing, responding to, and recovering from information security incidents.

14.2 All personnel and relevant third parties shall promptly report actual or suspected information security incidents through approved channels.

14.3 Security incidents shall be assessed and prioritized according to their potential impact and urgency.

14.4 Responsibilities and authorities for incident response shall be defined and communicated.

14.5 Information and evidence related to security incidents shall be appropriately protected and handled.

14.6 Significant incidents shall be escalated and communicated to relevant internal or external parties where required by applicable requirements or contractual obligations.

14.7 Lessons learned from incidents shall be used to improve information security controls and prevent recurrence.

15. Supplier and Third-Party Security:

15.1 Information security requirements shall be considered when selecting, evaluating, contracting, and monitoring suppliers and third parties that access the Company's information, systems, facilities, or other associated assets.

15.2 Appropriate information security, confidentiality, and data protection requirements shall be incorporated into contracts and agreements where applicable.

15.3 Third-party access shall be authorized, limited to legitimate business requirements, appropriately protected, and removed when no longer required.

15.4 Suppliers and third parties shall be monitored and evaluated according to the security risks associated with the services or resources provided.

15.5 Information security requirements shall be considered when acquiring or using externally provided services, systems, technology resources, or other relevant solutions.

15.6 Where third parties process information on behalf of the Company or its customers, appropriate security, confidentiality, privacy, and contractual requirements shall be established.

16. Secure Development and Change Management

16.1 Information security requirements shall be considered, where applicable, during the acquisition, development, implementation, modification, and retirement of information systems, applications, technology resources, and services.

16.2 Security requirements shall be identified and addressed before implementing or significantly modifying information systems or resources, where applicable.

16.3 Changes to information systems, applications, networks, infrastructure, and other relevant resources shall be appropriately assessed, authorized, tested, documented, and implemented through an approved change management process.

16.4 Development, testing, and production environments shall be appropriately segregated where applicable and based on risk.

16.5 Test data and environments shall be appropriately protected according to the sensitivity of the information.

16.6 Where software or systems are developed or customized by the Company, appropriate security practices, testing, vulnerability assessment, and code review shall be applied based on risk.

16.7 Where third-party software, components, or technology resources are acquired, appropriate security requirements shall be considered during selection and implementation.

17. Privacy and Protection of Personal Data:

17.1 Where the Company collects, processes, stores, transfers, or otherwise handles personal data, such activities shall comply with applicable privacy and data protection requirements.

17.2 Personal data shall be collected, processed, stored, transferred, retained, and disposed of only for authorized and legitimate purposes.

17.3 Appropriate technical and organizational measures shall be implemented to protect personal data against unauthorized access, disclosure, alteration, loss, destruction, or other unauthorized processing.

17.4 Access to personal data shall be limited to authorized personnel with a legitimate business need.

17.5 Where third parties process personal data on behalf of the Company, appropriate contractual, privacy, and security requirements shall be established.

17.6 Personal data shall not be disclosed, transferred, or processed outside authorized purposes or approved arrangements.

18. Audit, Assessment, and Compliance:

18.1 Information security compliance shall be periodically evaluated through audits, assessments, reviews, monitoring, and other appropriate activities.

18.2 Audit and testing activities shall be authorized, planned, and conducted in a controlled manner to prevent unnecessary risks to information systems and information.

18.3 Access provided for audit and testing purposes shall be limited to authorized personnel and appropriate timeframes.

18.4 Production systems shall not be subjected to intrusive testing without appropriate authorization and safeguards.

18.5 Asbab Technical Company shall identify and comply with applicable legal, regulatory, statutory, contractual, privacy, and information security requirements.

18.6 Nonconformities, security weaknesses, and identified areas for improvement shall be appropriately addressed and monitored to completion.

19. Policy Exceptions:

19.1 Any exception to this policy shall be formally documented, justified, risk assessed, and approved by the appropriate authority.

19.2 Exceptions shall have a defined validity period and shall be periodically reviewed.

19.3 Appropriate compensating controls shall be implemented where necessary to reduce the associated risk.

20. Monitoring, Review, and Continual Improvement

20.1 Compliance with this policy shall be monitored through appropriate reviews, audits, assessments, security monitoring, performance indicators, and management oversight.

20.2 The effectiveness of information security controls shall be periodically evaluated.

20.3 This policy shall be reviewed at least annually and whenever significant changes occur in the Company's activities, information assets, technology, risks, or applicable requirements.

20.4 The Information Security Management System and its controls shall be continually improved based on risk assessments, incidents, audit results, performance information, lessons learned, and changes in the Company's context.

21. Roles and Responsibilities

21.1 Top Management

Top Management shall:

- Approve and support the Information Security Policy.
- Provide appropriate resources and support for information security.
- Ensure that information security objectives are aligned with the Company's objectives.
- Ensure that significant information security risks are appropriately managed.

21.2 Information Security Function

The Information Security Function, or the person assigned responsibility for information security, shall:

- Coordinate the implementation and maintenance of the ISMS.
- Maintain information security policies and supporting requirements.
- Coordinate information security risk assessments and treatment.

- Monitor compliance and information security performance.
- Coordinate security awareness activities.
- Support incident management and security investigations.
- Report significant information security risks and performance to management.

21.3 IT / Relevant Technical Function

The IT or relevant technical function shall, where applicable:

- Implement and maintain applicable technical security controls.
- Manage relevant systems, infrastructure, networks, applications, and technical configurations.
- Support access management, backup, patching, vulnerability management, monitoring, and recovery activities.
- Implement approved technical security requirements.

21.4 Information and Asset Owners

Information and Asset Owners shall:

- Identify and classify information and associated assets.
- Define appropriate protection and access requirements.
- Approve access according to business needs.
- Participate in risk assessments and security reviews.

21.5 Employees and Contractors

Employees and contractors shall:

- Comply with this policy and applicable security requirements.
- Protect information and assets under their responsibility.
- Use organizational systems and information appropriately.
- Complete required security awareness and training.
- Report actual or suspected security incidents promptly.

21.6 Third Parties

Third parties shall:

- Comply with applicable contractual and information security requirements.
- Protect Company information and other information accessed or processed during service delivery.

- Report security incidents affecting Company information or services.
- Cooperate with security assessments where contractually required.

22. Enforcement:

22.1 Failure to comply with this policy may result in appropriate corrective, disciplinary, contractual, or legal action in accordance with applicable requirements.

22.2 Asbab Technical Company reserves the right to monitor the use of its information systems and associated assets to the extent permitted by applicable laws and regulations.

22.3 Serious or repeated violations shall be escalated to the appropriate management and relevant functions.