ADVANCED
TECHNOLOGY
SERVICES

Information Security Policy

BIM Group of Companies

G-103&105, Tower (E), Ground floor, Diamond
Condo, Kamayut Tsp, Yangon, Myanmar.

M: +959799476854 | E: info@bimats.com

W: https://www.bimgoc.com | L: BIM | F: BIM

BIM Group - "Digitally Transforming Your Business"

Change Log/ Version History

No.	*Version*	*Prepared by*	*Date*	*Remarks*
1	V 1.0	BIM Cybersecurity	5-Jun- 2021	Initial Document
2	V 2.0	BIM Cybersecurity	30 – Jun- 2021	Modified Version

Document Signed Off Sheet

Reviewed by:	Approved by:
Htun Win Naing	**Zay Yar Phyoe**
Executive Director	Managing Director
BIM Advanced Technology Services	BIM Advanced Technology Services

Table of Contents

Confidentiality Notice: This document is confidential and contains proprietary information and intellectual property of BIM Group of Companies. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of BIM Group of Companies. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited.

1. Introduction

1.1 Purpose

This document defines the BIM ATS's position on information security. The policy is applicable across the Company and is also subject to amendment at any time depending upon the changes in business requirements or environment with requisite approvals.

The objective of this policy is to describe the security requirements for information assets belonging to BIM Advanced Technology Services, used across the company. These assets can be in written, spoken or computer-based form and the protection and security of these assets from unauthorized disclosure, misrepresentation, loss, or wrongful use is of vital importance. Management and staff must ensure the Confidentiality, Integrity, and Availability of all information assets, as required.

The information security policy as stated in this document supports the following three objectives-

- Provide management direction and support for information security.
- Support the security requirements of the business and,
- Build business partnership/relations confidence.

1.2 Scope

The scope of the Information Security Policy is as specified in the Scope Document (***BIMATS_ ISMS_Scope***).

1.3 Owner

The senior manager is the owner of this policy and will be responsible for reviewing and updating the policy as and when required based on the change in the business requirements or environment. The manager will also ensure that the updated policy is implemented across the organization.

1.4 Document Structure

This document is structured and referenced following the 14 security categories of ISO 27001 standard:

- Information Security Policies
- Organization of Information Security
- Human Resource Security

- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operation Security
- Communications Security
- System acquisition, development, and maintenance
- Supplier relationships
- Information Security Incident Management
- Information Security aspects of Business Continuity Management
- Compliance

2. Information Security Policy

Objective: To ensure management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2.1 Information Security policy document

- The information security policy provides management direction and support to information security.
- The information security policy communicates throughout the organization to users in a form that is relevant, accessible, and understandable to the intended audience.
- The policy explains the policies, principles, and compliance requirements for particular importance to the organization, including:
  - Legislative, regulatory, and contractual compliance.
  - Security education, training, and awareness requirements.
  - Business continuity management and
  - Consequences of information security policy violations.

2.2 Information Security Policy for BIM Advanced Technology Services

BIM Advanced Technology Service's Information Security Policy commits the Company to protect the security of its information. It provides the same commitment to information entrusted BIM Advanced Technology Services by its customers and business partners. We will deliver the above components in an integrated manner through an Information Security Management System that protects the Confidentiality, Integrity, and Availability of BIM Advanced Technology Service's information.

To meet this commitment, BIM ATS follows these procedures:

- Maintain an effective Information Security Management System
- Deploy most appropriate technology and infrastructure.
- Create and maintain a security conscious culture within Information Services
- Continually monitor and improve the effectiveness of the information Security Management System.

Responsibility for compliance with BIM Advanced Technology Service's Policy and standard lies with senior manager and their staff.

2.3 Review of the policies for information security

Objective

Information Security Reviews are necessary to identify and document unmitigated risks that may exist on new or existing BIM Advanced Technology Service information systems or information technology (IT) solutions and provide recommendations to mitigate the identified risk. Information Security Reviews must be performed whenever new IT services or equipment are acquired or when significant changes are made to existing systems, infrastructure, or services. An Information Security Review, along with the recommended security controls, work to improve the BIM Advanced Technology Service's security posture.

Information Security Review Policy

Information Security Reviews must be performed in the following scenarios:

- Implementation of new information services and systems; or significant changes to existing BIM Advanced Technology Service information services or systems, that may store or transmit Export Controlled or Restricted data.
- Implementation of new critical infrastructure or significant changes to existing critical infrastructure.
- Implementation of a new enterprise system or significant changes to existing enterprise systems.
- Implementation of new systems or significant changes to existing systems, which permit third party access to BIM Advanced Technology Service systems or data.
- Implementation of cloud services for the storing or processing of Export Controlled, Restricted or Controlled data.

3. Organizational Security

3.1 Internal Organization

Objective:

- Establishing a management framework to initiate and control the implementation of information security within the organization.
- Ensuring that a governance framework is developed to maintain information security within the organization and
- Assigning the security roles and coordinating the implementation of security across the organization.

Management approves the information security policy, assign security roles and co-ordinate, and review the implementation of security across the organization.

3.1.1 Information Security Coordination

Company management ensures an effective coordination of information security activities across the organization between various department including Human Resources, Information Technology, Legal, Finance and Business Operations and **BIMATS_SOC Incident Management Procedures** and **BIMATS_Business Continuity Plan** documents. The activities ensure that:

- All non-compliances to information security policy are addressed.
- Significant changes in threats and exposure to information and information processing facilities are identified and
- Information security incidents are identified and addressed appropriately.

3.1.2 Coordination with special interest parties

To stay up to date about latest technologies, BIM ATS must maintain the relationship with other security specialist communities and professional associations. The goal is to

- Improve knowledge about best practices and stay up to date with relevant security information.
- Receive early warnings of alerts, advisories and patches concerning to attacks and vulnerabilities.

- Share and exchange information about new technologies, products, threats, or vulnerabilities.

3.1.3 Allocation of information security responsibilities

- Information security roles and responsibilities for the member of BIM ATS (Advanced Technology Service) will be clearly defined and documented.
- Information asset owners responsible for the security of the information asset and for identifying and implementing the controls that are necessary to protect the asset.
- The senior manager performs the quarterly compliance checks, or get it carried out by trusted third parties, to ensure that all information security policies and processes are compiled by across the organization.

3.1.4 Authorization process for information processing facilities

- A formal risk assessment is performed and approved by the BIM ATS for new technologies used in the Company production information system.
- Any infrastructure updates or changes made within the BIM ATS will not be performed without confirmation of responsible personnel from BIM ATS.
- Critical components of the Company's information security infrastructure will not be disabled, bypassed, turned off, or disconnected without prior approval from management team from BIM ATS.

3.1.5 Confidentiality agreements

- User sign Non-Disclosure Agreement highlighting confidentiality requirements as part of their initial terms and conditions of employment.
- Without specific written exceptions, all programs and documentation generated by, or provided by and employee for benefit of the Company are the property of the Company and all employees providing such programs or documentation will sign a statement to this effect prior to the provision of these materials.
- Whenever communications with third parties necessitate the release of the Company's sensitive information, a standard Non-Disclosure Agreement (NDA)

or confidentiality clause, authorized by the Company's Legal department, will be signed by the third party.

3.1.6 Independent review of information security

- An independent review of information security policy and associated controls will be performed as stated in section 2.3 and the Internal security review must perform every six months.

3.2 External parties

3.2.1 Identification of risks related to external parties

The risks associated with access to the Company's internal systems by third parties will be assessed and appropriate security controls implemented. When using an external contractor to manage information processing facilities, risks will be identified in advance, mitigating controls will be identified and established, and contractor expectations will be incorporated into the contract for these services.

3.2.2 Addressing security when dealing with customers

- The level of required for the customers and the list of users requiring access.
- Justification, requirements, and benefits for customer access.
- The contractual right to monitor, revoke any activity related to company assets.
- Respective Liabilities of the organization and the customer; and
- The above-mentioned requirements shall be documented and signed by the customer and company. These requirements shall be incorporated in the contractual agreement with the client.

The company will not publicly disclose any information related to business deal or transaction that could reasonably be expected to be materially damaging to a customer or another third party.

3.2.3 Addressing security in third-party agreements

- The security requirements of outsourcing the management and control of all or some of the Company's information systems, networks and/or desktop environments are addressed in a contract agreed between the parties.

3.3 Mobile Devices and Teleworking

3.3.1 Mobile Device Policy

- Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by BIM ATS IT Team.
- Any mobile device that is used to conduct BIM ATS's business should be used appropriately, responsibly, and ethically.
- Any BIM ATS employees are responsible for using a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied.

3.3.2 Teleworking

Employees from BIM ATS must:

- Keep their equipment password protected.
- Store equipment in clean and safe place when not in use.
- Follow all data encryption, protection, standards, and settings.
- Refrain from visiting untrustworthy or suspicious sites.
- Only download authorized software with approval from EUC Team from BIM ATS.
- Keep confidential information in locked file cabinets and desks.

4.Human Resources Security

Objective: The Employees must understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities.

4.1 Prior to employment

All offers of employment at BIM_ATS are contingent upon clear results of a thorough background check. Background checks will be conducted as stated in the **"BIMATS_Background Check Policy and Procedure"** document, on all final candidates and on all employees who are promoted, as deemed necessary.

4.1.1 Roles and responsibilities

- Users are needed to fulfill all security roles and responsibilities as laid down in this Information Security Policy.

4.1.2 Screening

The scope of screening is clearly defined in the Scope Document (***BIMATS_Background_Check_Policy&Procedure***).

Background screening, as required for the role, on permanent staff is carried out at the time of job applications. A similar screening process is carried out or incorporated as part of the contract for contractors and temporary staff in accordance with the Risk Assessment of the External Parties. Information systems technical details, such as network addresses, network diagrams, and security software employed, cannot be revealed to job applicants until they have been hired and have signed a confidentiality agreement. Persons who have a criminal conviction are not hired into, retained for, promoted into, or maintained in computer-related positions of trust.

4.1.3 Terms and conditions of employment

The terms and conditions of employment includes the employee's responsibilities for information security as laid down by the Information Security Policy. Employees of the Company grant the Company exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop.

4.2 During employment

4.2.1 Management responsibilities

- Management is required employees, contractors, and third-party users to apply security in accordance with Company's established policies.
- Management ensures that Function Heads are responsible for promoting security across their departments.
- Function Heads ensures that information security within their departments is treated as mandatory and employees are encouraged to adhere to Company's information security policies.

4.2.2 Information security awareness, education, and training

- All employees of the organization and where relevant, third-party users receive appropriate training and regular updates in organization policies and procedures.
- All employees must attend security awareness training which conducts annually and pass the security awareness exam with a score of 80%.

4.2.3 Disciplinary process

- The violation of organization security policies and procedures by employees is dealt with rules and procedures of existing BIM Advanced Technology Service's Conduct, Discipline and Appeal Rules and modified standing Order.

4.3 Termination or change of employment

4.3.1 Termination responsibilities

- Human Resources notify IT department and all other stakeholder (from support and business functions) about the transfer or termination of any employee and any other third-party personnel or contractors of the organization without delay.
- Unless the IT departments has received instructions to the contrary, within 30 days after an employee has permanently left the Company, all files held in that user's directories will be purged unless reporting manager needs that data.
- The system user IDs are disabled for a period of one month after and employee has permanently left the Company.

- Employee must sign off the "**BIMATS_Employee Exit Clearance Checklist** Document."

4.3.2 Removal of access rights

System privileges and access to information and information assets of an employee will be removed within 72 working hours after receiving mail from personnel department.

5. Asset management

Objective: To ensure and maintain appropriate protection of organizational assets.

5.1 Inventory of assets

- For each of the identified assets, ownership of the asset should be assign as stated in section 5.1.2 and category should be identified as stated in clause 5.2.
- Information assets at the Company will be classified based on the impact in the organization, due to loss of their confidentiality, availability, and integrity.
- An Inventory if all critical information asset will be drawn up and maintained to ensure appropriate protection of Company's information assets. The inventory shall include all information necessary to recover from disaster, including type of asset.

5.1.2 Information Owners

- An owner will be identified for each of the information assets at the Company. The owner will be responsible for:
  - Ensuring that information and assets associated with information processing facilities are appropriately classified; and
  - Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies.
- Information Asset owners or their delegates are responsible for the following activities:
  - Approve information-oriented access control privileges for specific job profiles.

  - Approve information-oriented access control requests that do not fall within the scope of existing job profiles.
  - Select special controls need to protect information, such additional input validation checks, or more frequent backup producers.
  - Define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage.
  - Approve all new and different uses of their information.
  - Approve all new substantially enhanced application systems that use their information before these systems are moved into production operational status.
  - Review reports about system intrusions and other events that are relevant to their information.
  - Select a sensitivity classification category relevant to their information, and review this classification every year for possible downgrading or upgrading; and
  - Select a criticality category relevant to their information so that appropriate contingency planning can be performed.
- Information Owners will designate a back-up person to act if they are absent or unavailable. Owners will not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time employee of the Company.

5.1.3 Information Custodian

- The information asset owner will identify a custodian for information asset.
- The Custodian is in physical of logical possession of information and information systems and will perform the following activities:
  - Following the instruction s of Owners, operation systems on behalf of Owners to serve users authorized by Owners.
  - Define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information.

- Define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to optimal business objectives.
- If requested, provide reports to Owners about information system operations and information security issues; and
- Safeguard the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

5.1.4 Acceptable use of assets

All employees have a personal responsibility for safeguarding all proprietary information, which includes but is not restricted to Sensitive documents and information, from disclosure to unauthorized parties.

5.1.5 Return of assets

Company property including, but not limited to, portable computers, library books, documentation, building keys, magnetic access cards, etc. will be returned at the time when an employee leaves the organization. Employees are mandated to get sign off from the following department (but not limited to) on the no dues/ clearance from (BIMATS_Employee Exit Clearance Checklist Document) after return of assets:

- Finance
- Administration9
- Human Resources
- Legal

5.2 Information classification

5.2.1 Classification guidelines

- Information assets of the organization are classified based on their relative business value, legal requirements, and impact due to loss of confidentiality, availability, and integrity of the information asset.
- The level of security is identified based on the information classification performed which is stated in section 6.1.1.
- Asset are grouped under the following asset types:
  - Physical assets
  - Software assets
  - Information assets
  - Services assets
  - People assets
- The information assets are classified in the following four categories:
  - **Restricted:** Information that is highly sensitive and is available only to specific, named individuals (or specific positions).
  - **Confidential:** Information that is sensitive outside the Company/Business and available only to a specific function, group, or role.
  - **Internal:** Information that is sensitive outside the Company/Business and needs to be protected. Authorized Access to employees, contractors, sub-contractors, and agent on a "Need to Know Basis" for Business related Purposes.
  - **Public:** Public Information (including information deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors, and agents.
- If information is not marked with one of these categories, it will default into "internal" category.

5.2.2 Information Labelling and handling

- The owner or creator of information is needed to assign an appropriate label to the information, and the user or recipient of this information also need to consistently maintain an assigned label based on the classification of the information as stated in the section 5.2.1.
- Labels for sensitive information appear on the outside of CD-ROMs, Flash drives and other storage media. If a storage volume such as a Flash drives contains information with multiple classifications, the most sensitive category will appear on the outside label.
- Making additional photocopies or printing extra copies of information classified as 'Sensitive' information will not take place without the prior permission/ approval of the Information Owner.
- Sensitive information on paper such as print outs, writing, fax etc. is personally delivered to the designated recipients. Such output will not be delivered to an unattended desk or left out in open in an unoccupied office.

6. Access Control

Objective: To limit access to information and information processing facilities.

6.1. Business requirement for access control

6.1.1 Access control policy

While establishing these polices, BIM ATS considers both logical and physical access controls as stated in the clause 8.

- BIM ATS ensures that access to its information and business processes is controlled according to the business and security requirements.
- Access to Public and Internal Use Only information is not restricted with access controls that discriminate by specific user depending on the classification of the information as stated in the section 5.2. 1. For example, public information is available at the BIM ATS's website, and Internal Use Only information is available on the Company's internal SharePoint.
- Access to Sensitive information is granted only when a legitimate business need has been demonstrated and access has been approved in advance by the Information Owner.
- Users are responsible for all activity that takes place with their user ID and password or other authentication mechanism.
- A user is needed to change their password immediately if they suspect that it has been discovered or used by another person and report this to the respective engineers as stated in the section 12.1.
- Employees cannot use Company information systems to engage in hacking activities that include, but are not limited to, gaining unauthorized access to any other information systems damaging, altering, or disrupting the operations of any other information systems and capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.
- Employees cannot change or update information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved declassification process.

6.1.2 User Management

- All user IDs on Company computer and networks are constructed according to the Company standard user ID construction, which are used to clearly indicate the responsible individual's name and under no circumstances are such user IDs will be permitted to be generic, descriptive of an organizational title or role, descriptive of a project, or anonymous.
- Every user has a single unique user ID and a personal secret password for access to the Company multi-user computers and computer networks.
- There are formal user access creations and deletion procedures for granting access to all multi-user information systems and services.
- User creation or de-creation/ modification request is required to be authorized by the line manager and submitted to respective personnel before user access is created as stated in the section 6.1.4.

6.1.3 Privilege Management of employees

- An employee's manager initiates the access control approval process, and the privileges granted remains in effect until the employee's job changes or the employee leaves Company. If either of these two events occurs, the manager will notify the IT department immediately.
- The computer and communications system privileges of all users, systems, and programs is restricted based on the need to know.
- All other system capabilities are provided through job profiles or by special request approved by the involved Application Owner.
- Employees who are assigned high level privileges will use a different login for normal business use (e.g., "System Administration" login must not be used for checking e-mail).
- Privileges will be granted on the server after adequate approval from the senior line manager.
- The privileges associated with each application as well as the role to which they need to be allocated will be identified and documented.

6.1.4 Review of user access rights

- All user IDs have the associated privileges revoked after a 60-day period of inactivity.

- Verify that the level of access is granted is appropriate to the access policies as stated in the section 6.1.1 and it is consistent with other requirements such as segregation of duties as stated in the section 3.1.3.
- The system access history and user logs are reviewed periodically by the IT department. Redundant and unused user accounts are removed on a quarterly basis.
- Management conducts a formal review of users' access rights twice in a year.

6.2 User responsibilities

6.2.1 Password use

- Users are not allowed to employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of speech.
- Passwords are not allowed to share or reveal to anyone other than the authorized users.
- Users are not allowed to store fixed passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software.
- Passwords cannot be written down unless a transformation process has concealed them, or they are physically secured, such as placed in a locked file cabinet.

6.2.2 Unattended user equipment

- Personal computers, computer terminals and printers cannot be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism when unattended and will be protected by key locks, passwords, and other controls when not in use.

6.2.3 Clear desk and clear screen policy

- BIM ATS has a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.
- Outside of regular working hours, all employees must clear their desks and working areas from all sensitive or valuable data.

- When not in use, sensitive information left in an unattended room is locked away in appropriate containers.

6.3 Network access control

6.3.1 Policy on use of network services

- Users have direct access to the services that they have been specifically authorized to use as stated in the section 6.1.1.
- Users cannot establish any external network connections that could permit third party users to gain access to Company systems and information unless prior approval from internal IT department has been obtained.
- When using Company information systems, or when conducting Company business, users will not deliberately conceal or misrepresent their network identity.

6.3.2 Remote diagnostic and configuration port protection

- Access to all diagnostic ports is provided after approval from the senior manager. Connection to the remote diagnostic ports is provided using secure communication channels.

6.3.3 Segregation in networks

- Every sensitive and high-reliability system managed by or owned by the Company has its own dedicated computers and networks, unless approved in advance by the senior manager.

6.3.4 Network routing control

- All Company internal networks are divided into security zones wherever appropriate.
- All Company internal networks have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.

6.4 Mobile computing

6.4.1 Mobile computing and communications

- Users cannot store passwords, user IDs, or any other access information in portable or remote systems.

- Users need to be careful not to discuss sensitive information when in public places like hotel lobbies, restaurants, and elevators etc.
- Viewing sensitive information on a computer screen or hardcopy report is prohibited when a user is in a public place such as seated on an airplane.
- Users can only be provided sensitive information in voice mail messages or alphanumeric messages.
- When using public Internet terminals to check email, users must log out correctly from Company systems when finished.

6.5 System and Application Access Control

Access to BIM systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized use or access of the organization's information systems.

6.5.1 Information Access Restriction

- Only the authorized users are allowed to access the implemented systems for each business functions such as invoice system, billing system, sales pipeline.
- The system administrator will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
- The permission access rights (Read/Write/Edit) must be classified and assigned regarding the roles and responsibilities of the privilege user.
- The list of users and the access rights must be documented and must be reviewed periodically for the user access rights.
- It is not allowed to use shared accounts for accessing the systems and applications.
- Audit trails of system and user activity in the systems are to be produced.

7. Physical and Environmental Security

Objective: To ensure and prevent unauthorized physical access, damage, and interference to the organization's premises and information.

7.1 Secure areas

7.1.1 Physical security perimeter

- All multi-user computer and communications equipment is held in a room with adequate access control mechanism installed. E.g.: figure prints or a proximity cards access.
- Every company multi-user computer and communications facilities have physical security plan that is reviewed and updated annually by the line admin in charge of facility.

7.1.2 Physical entry controls

- Access to every office, computer room, and work area containing sensitive information is physically restricted to limit access to authorized personnel only.
- All persons wears and identification badge on their outer garments ensuring that both the picture, in case of employees, and information on the badge are clearly visible whenever they are in Company secure buildings or facilities.
- Employees are not permitted unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when they go through these entrances.
- Visitor or other third-party access to Company offices, computer facilities, and other work areas containing sensitive information will be controlled by guards, receptionists, or other staff.
- Access permission to secure area should be regularly reviewed and updated or even revoked, if necessary, as stated in the sections 6.1.2 and 6.1.4.

7.1.3 Securing offices, rooms, and facilities

- There are no signs indicating the location of computer or communication centers.
- Multi-user computer and communications facilities (including telephone closets, network router and hub rooms and similar areas containing computer and / or communications equipment) is kept always locked and

not be accessible by visitors without authorized IT staff escort to monitor all work being performed.

7.1.4 Protecting against external and environmental threats

- Local management provides and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environments protection systems in Company multi-user and personal computer facilities.
- All openings to walls (such as doors and ventilation ducts) surrounding multi-user and personal computer facilities is made for self-closing.

7.1.5 Working in secure areas

- The main multi-user and personal computer facility is always staffed by technically competent staff 24 hours a day, seven days a week, 365 days a year.
-
- Employees and visitor are not allowed to smoke in multi-user and personal computer facilities.

7.1.6 Public access, delivery and loading areas

- A secured intermediate holding area is used for computer supplies, equipment, and other deliveries.
- Any incoming assets should be registered to be able to align with the asset management procedure as stated in the clause 5.

7.2 Equipment security

7.2.1 Equipment sitting and protection

- All elements of production computer systems including, but not limited to, servers, firewalls, hubs, and routers etc. is physically located within a secure area and labeled by using bar code.
- The physical address of every Company multi-user and personal computer facility is confidential and is disclosed to unauthorized individuals.

7.2.2 Supporting utilities

- All network equipment is fitted with uninterruptible power supply system's electrical power filters, or surge suppressors that have been approved.
- All Company multi-user and personal computer have alternative source of power, such as Generator sets etc., so that normal business operations are

sustainable even during extended period of unavailability of main power supply.

7.2.3 Cabling security

- Power and telecommunications cabling carrying data supporting information services is protected from interception of damage.
- Cabling of Company's internal network is physically protected from any damage or vandalism by lying in plenum spaces.

7.2.4 Equipment maintenance

- Preventative maintenance is regularly performed on all computer and communications systems.
- All hardware and software products are registered with the appropriate vendors for maintenance, after Company staff takes delivery of new or upgraded information systems products.
- The Annual Maintenance Contracts for all hardware and software products, if applicable, is monitored and reviewed after every six months.

7.2.5. Security of equipment off-premises

- Any use of equipment for information processing outside company premises requires authorization by management. Authorization for issue of mobile computing devices (laptops) consider as an authorization for use of equipment for information processing outside Company premises.
- Employees store mobile phones and other hardware sensibly and securely when storing outside Company's premises e.g., hotels, airports. Equipment will not be left unlocked, logged in or powered up without the employee being with the equipment.

7.2.6. Secure disposal or re-use of equipment

- Information is set to erased from equipment prior to disposal or re-use.
- Equipment is disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities, or commercial organizations.

7.2.7. Removal of property

- Equipment, information, or software belonging to the organization cannot removed without authorization of the relevant departmental manager.

8. Communications and Operations Management

Objective: To ensure the correct and secure operation of information processing facilities.

8.1 Documented operating procedures

- Company IT project delivery department, after the approval from the senior manager, may, at any time, alter the priority, or terminate the execution of any user process that is consuming excessive system resources or is significantly degrading system response time, after a prior authorization.
- Company IT project delivery department staff is allowed to terminate user sessions or connections if the usage is deemed to be in violation of security policy.
- At all times, at least two IT project delivery department personnel can provide any given essential technical service (irrespective of the local/remote) for information systems critical to business during office hours.
- The operating procedures are documented, maintained, and made available to all users who need them and will include:
  - backup procedure
  - incident management procedure as stated in the clause 12.
  - support contacts in the event of unexpected operational or technical difficulties
  - job scheduling
  - system start-up and shutdown procedure; and
  - management of audit-trail and system log information.

8.2 Change management

- All production computer and communications systems at the Company employ a formal change management procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.
- Changes to all information processing facilities and systems is controlled and documented to ensure that any changes and additions do not compromise information security.

- The details of all the changes approved and performed is allowed to communicate to all the relevant persons or departments.

8.3. Segregation of operation

- All the mutually exclusive roles and corresponding access permissions are identified and reviewed annually.
- Whenever a Company computer-based process involves sensitive information, the system includes controls involving separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information assets.

8.4 Protection from Malware

8.4.1. System acceptance

Before computer systems and network segments can be connected to the Company network, they will meet the security criteria established by BIM ATS including, but not limited to

- latest OS patches
- anti-virus with latest definition
- local admin password change; and
- host name.

8.5 Backup

8.5.1 Information Backup

- All user level and system level information maintained by BIM ATS must be backed up periodically.
- The frequency and extend of backup must be in accordance with the importance of the information as stated in the section 5.2 and acceptable risks determined by the owner.
- Backed up data must be tested to ensure that they are recoverable

8.5.2 Data Recovery

- Determine which information need to be restored and in what order according to the importance of the data as stated in the section 5.2.

8.6 Logging and Monitoring

BIM ATS EUC team is responsible for monitoring and logging all the physical assets such as routers and computers.

8.7 Control of operational software

- All employees are responsible for not installing software without prior notice of BIM ATS's EUC team acknowledgement.
- Mobile devices should be restricted from installing unauthorized software through proper technical configuration.

8.8 Technical Vulnerability Management

- Security testing and technical vulnerability scanning of BIM ATS applications, operating systems and network devices must identify new technical vulnerabilities and provide a view of vulnerabilities across the organization's technical infrastructure
- This action must be performed on a regular basic informed by the risk function and in compliance with the company's policy.
- Software should be restricted from being installed as stated in the section 9.7.

8.9 Information System Audit Consideration

- Security audits will be conducted annually to ensure information system security controls have been implemented correctly, are operating effectively, and are producing the desired level of security.
- Audit personnel must be independent of the activities being audited
- The resources performing the checks must be explicitly identified.
- Existing security measures will be used when possible.
- All-access must be monitored and logged, and all procedures, requirements and responsibilities must be documented
- Audit tests that could affect system availability must be run outside business hours
- Appropriate personnel must be notified in advance to be able to respond to any incidents resulting from the audit.

8.10 Network security management

8.10.1 Security of network services

- Network services are set only to accept communications from authenticated sources.
- All connections between Company internal networks and the Internet or any other publicly- accessible computer network includes an approved firewall and related access control system.
- The privileges permitted through this firewall or related access control system is based on business needs and defines in an access control standard issued by the BIM ATS member.
- Firewall configuration rules and permissible service rules cannot be changed unless the permission of the senior manager has been obtained.
- Wireless networks used for Company transmissions is configured to employ appropriately configured encryption.
- Wireless network gateways are configured so that they employ firewalls to filter communications with remote devices.
- Wireless technology cannot be used for the transmission of unencrypted Sensitive information.

.

8.11 Exchange of information

8.11.1 Electronic messaging

- Company system administrators needs to maintain electronic mail messages and accompanying logs as per backup management procedure.
- Employees cannot employ any electronic mail addresses other than official Company electronic mail addresses for all company business matters.
- Unless the Information Owner or originator agrees in advance, or unless the information is clearly public in nature, employees cannot forward electronically mail to any address outside of the Company network.
- Employees cannot create and send, or forward externally provided electronic mail messages that may be harassment or that may contribute to a hostile work environment.

- An electronic mail message is retained for future reference if it contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a Company management decision.
- Employees cannot monitor electronic mail systems for internal policy compliance, suspected criminal activity, and other systems management reasons unless electronic mail monitoring tasks have been specifically delegated and approved by the Function Heads and Human Resources.
- Employees cannot send or forward any messages through Company information systems that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone based on race, gender, national origin, sexual orientation, religion, political beliefs, or disability.
- Employees cannot use Company computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients.
- When employees receive unwanted and unsolicited electronic mail, they forward the message to the electronic mail administrator and cannot respond directly to the sender.
- Users who receive an unexpected attachment to an electronic mail message that does not have a credible business-related explanation cannot open the attachment until they obtain an explanation from the sender.

8.12 Electronic commerce services

8.12.1 Publicly available information

- Every public written use of the Company name in published material requires the advance approval of a Company Director or the Corporate Communications department.
- Employees cannot misrepresent, obscure, suppress, or replace their identity on any electronic communications.
- Unofficial comments that users post to an electronic mail system, an electronic bulletin board system, or other electronic systems cannot be considered as formal statements of or the official position of the Company and cannot be made from Company systems.

9. Information Systems Acquisition, Development and Maintenance

9.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems across the entire lifecycle. The requirements for information systems which provide services over public networks is also included in this section.

9.1.1 Security requirements analysis and specification

- Before a new system is developed or acquired, the responsible line manager must clearly specify the relevant security requirements. (e.g., Threat Modelling, Incident Reviews and Use of vulnerability thresholds.)
- Business requirements for new systems or enhancements to existing systems must be specified the required security controls. (e.g., Deriving compliance requirements from policies and regulations)
- Every result of the identification must be documented and reviewed by the project managers and management team.
- The project manager or coordinator must be assigned the role and responsibilities of the project delivery team internally and informed or acknowledge project information to the users or customers.
- The project owner must require protect the project information or customer data, which is regarding availability, confidentiality, integrity. The initial risk assessment report must send to the senior management team by project manager monthly to reduce the risk of the delivering project.
- The initial requirements checklist must prepare and assessed in the Azure Devops of Software Development Environment for each customer must be implemented to fulfill the business requirements such as transaction logging and monitoring, nonrepudiation requirements.
- The software developers and system owners must be enabled the security controls, permission of the software repository. The security control checklist report must be review by the project manager or information security officer to reduce the data leakage and make sure the logging and monitoring of the software development repository in Azure Devops environment.

9.1.2 Securing Application Services on Public Networks

System owners must consider following things for the application services when passing over public networks

- Improper implementation of least privilege.
- Software failures
- Authentication mechanisms are easily passed
- Improper error handling
- Improper input validation

System owners must act these things while securing application services on public networks

- System owners need to ensure the number of users with critical functionality and controls are restricted and it is implemented properly.
- Every data must be backed up periodically to mitigate unforeseen incidents
- Input validation must prepare the statements or stored procedures, disallowing dynamic query construction using input to defend against injection attacks
- Disallowing active scripting in conjunction with output encoding and request validation to defend against Cross-Site Scripting (XSS).
- The use of security zones must separate the different levels of access according to the zone that the software or person is authorized to access.

9.1.3 Protecting Application Services Transactions

- Authentication Modules must leverage directory services
- Authentication Modules must leverage access management software and services
- Logging modules must be to log message that are input into and output from the application
- Availability modules must monitor all the capacity, network flow, etc. Validation modules are also required to make sure the ingress and egress

filtering of messages that come into or leave the application. It needs to be used guarantee delivery of messages.

- Cryptographic modules must provide encryption, decryption and hashing services of application and securing database.

9.2 Security in development and support process

Objective: To ensure that information security is designed and implemented within the software development lifecycle of information systems.

9.2.1 Secure Development Policy

Secure Development Policy must cover up following things

- Securing Software Development Environment
- Patch Management
- Code Analysis
- Code Review (Peer Review)

9.2.2 System Change Control Procedures

Every change in system must be verified by following procedures

- Change requests are evaluated for impact on the overall security of the software
- The asset management database is updated with the updated software information
- The change is requested formally and evaluated and approved by appropriate signatory authorities
- System owner must ensure that the operation runs continuously and has no impact to the organization after the system changes

9.2.3 Technical Review of Application after operation platform changes

- Software development team must review when the operation platform changes need to be conducted is performed to ensure that the software performs as expect and meets business requirements and specifications.
- System owner and project manager must review and test to ensure that there is no adverse impact on the organizational operations or security.

9.2.4 Restriction on changes to software packages

- Newer versions of the software must be approved, tracked, and validated to ensure that the current state and level of security in the software has not been reduced.
- Changes must not be allowed unless the appropriate authorities formally approve the change.
- All changed need to be formally request to the project manager.

9.2.5 Secure system engineering principles

- BIM ATS Software development Team must apply and follow secure engineering techniques in the development of applications that have input and output interfaces under the secure engineering techniques on user authentication techniques, secure session control and data validation, sanitization, and elimination of debugging codes.
- Have knowledge of Standard security engineering principles (e.g. OWASP software security checklist, SANS dangerous programming errors)

9.2.6 Secure Development Environment

- Before the software is installed into the production environment, the host must be qualified to install (security perspective).
- Ensure that pre-installation checklists are satisfied to be able for the software to run properly
- Unnecessary data for outdated or expired software from the system must be disposed properly

9.2.7 System Security Testing

Security testing team must use testing tools to test-

- Static binary code
- Dynamic vulnerability scanning
- Security Compliance Validation

9.2.8 System Acceptance Testing

- Verify that the software meets specified functional and assurance requirements
- Verify that the software is operating completely and securely

- If the software is deployed internally, development team or system owner must state transference of responsibility

9.3 Test Data

Objective: To ensure the protection of data used for testing

9.3.1 Protection of test data

- The use of sensitive production data in non-production environments must be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval must be obtained from senior management
- Test data must be selected carefully, protected, and controlled
- Record and manage test data.
- All the approvals, documents, and controls for the use of live data in pre-production environments for the system must be recorded

10. Relation with suppliers

10.1 Information security in Supplier Relationships

Objective: To ensure protection of BIM's assets that is accessible by suppliers; and maintain an agreed level of information security and service delivery in line with supplier agreements.

- The security controls for suppliers/ vendors to meet the minimum-security expectations / requirements must be defined in the Service Level Agreement.
- Non-disclosure agreement must be agreed and signed by both parties, BIM, and suppliers to protect information.
- Proper procedures for handling, processing, storing, and communicating information must be defined.
- Types of information access that different types of suppliers will be allowed and monitoring and controlling the access must be defined
- Acceptable use of information, including unacceptable use of policy must be defined.
- The supplier processes and controls related to the agreement must be audited
- Rules for sharing of information regarding to the supply chain and any potential issues and compromises among BIM ATS and suppliers must be defined

10.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements

- Monitor service performance levels to verify adherence to the agreements
- Service reports produced by the supplier and arranged regular progress meetings as required by the agreement must be reviewed.
- Resolve and manage any identified problems

11. Information Security Incident Management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

11.1 Reporting information security events and weaknesses

11.1.1 Reporting information security events

- IT and Project Delivery Department establishes a framework for reporting, responding to escalating information security events configure the same in the incident management system.
- BIM Cybersecurity team are responsible for reporting all identified security events and incidents promptly to the responsible personnel from BIM ATS team as stated in the section 12.2.1.

11.1.2 Reporting security weaknesses

- Project delivery department establishes an incident management procedure for reporting, responding to an escalating any suspected security weakness or threat to systems or services.
- Users report all information security alerts, warnings and suspected vulnerabilities to the management, in a timely manner, and can share such information with only with authorized personnel.
- Employees promptly are aware to notify management of all conditions that could lead to a disruption of business activities.

11.2 Management of information security incidents and improvements

11.2.1 Responsibilities and procedures

- BIM Cybersecurity establishes a procedure to ensure an effective, timely and orderly response to information security incidents. Guidelines are established for collective and maintaining evidence collected as required by legislation.

11.2.2 Learning from information security incidents

- Information security incidents are monitored and analyzed 24/7 by BIM Cybersecurity.
- Incidents with high business impact are identified and appropriate controls will be enhanced to reduce the risk from future occurrences of such incidents.

11.2.3 Collection of evidence

- Where action against a person or organization involves the law, either civil or criminal, the evidence collection and presentation must conform to applicable laws. This will include compliance with any published standard or code of practice to produce admissible evidence.
- All investigations of alleged criminal or abusive conduct will be treated as restricted information to preserve the reputation of the suspected party until charges are formalized or disciplinary action taken.
- All internal investigations of information security incidents, violations, and problems are conducted by authorized staff.

11.3 Assessment and Decision on information security event

As stated in the **BIMATS_Incident Management Procedure** document, all the security events happen in BIM ATS will be taken actions by BIM Cybersecurity team.

12. Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Business process line owners are responsible for ensuring that the key events that can cause disruption to their processes are identified and their potential adverse impact, financial and non-financial, is documented.

The scope of the Business Continuity Plan considers applicable factors including customer requirements and legal regulations. The following facts are considered while implementing any DR / BCP program:

- Identity critical business functions, applications and supporting technologies.
- Identify alternate, backup locations with the necessary infrastructure to support the recovery needs
- Identify the management and membership of the disaster response and recovery teams
- Identify and document the required recovery actions, identify, and ensure the availability of required resources, and compile this information as the recovery plan
- Train the recovery team in the performance of their specific tasks
- Identify vendor recovery support capability
- Identify data protection and data recoverability status
- Identify functional team, recovery support and response capabilities and
- Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

12.2 Business Continuity and risk assessment

BIM ATS wants a strategic plan which is based on appropriate risk assessment is developed for the overall approach to business continuity. BIM ATS considers-

- Identify events that cause interruptions to business processes
- Consider all critical business processes, not just information processing facilities

12.3 Developing and implementing continuity plans including information security

All departments of BIM ATS establish and use a logical framework of classifying all information resources by recovery priority that will permit the most critical information resources to be recovered first.

All departments must prepare, periodically update, and regularly test the business recovery plan that specifies how alternative facilities will be provided so employees can continue operations in the event of a business interruption.

12.4 Business continuity planning framework

A single framework of business continuity plans will be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

12.5 Testing, maintaining, monitoring, and re-assessing business continuity plans

If critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan will be developed, tested periodically, updated, and integrated into computer and communication system contingency plans.

BIM ATS management team will annually revise and documenting the support levels that will be provided in the event of a disaster or emergency. Computer and communication system contingency plans are routinely tested and followed up with a brief report to BIM ATS management with detail results. Quarterly, emergency contact information will be validated and revised indicating for every employee involved in business continuity and disaster recovery planning and implementation. The roles and responsibilities for both information system contingency planning and information systems recovery will be reviewed and updated annually.

13. Compliance

Objective: To avoid breaches of any law, statutory, regulatory, or contractual obligations and of any security requirements as defined by BIM ATS's policy, procedure, standard and guideline.

13.1.1 Identification of applicable legislation

All relevant statutory, regulatory, and contractual requirements is defined explicitly and documented for all information processing facilities.

13.1.2 Intellectual Property Rights

BIM ATS will be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties.

- All intellectual property, such as documents, inventions which are developed by a user while employed by the Company, will be the property of the Company.
- At the time of termination of employee relationship with the Company, all employees will return any intellectual property provided or developed during the period of the that employee's employment.
- All BIM ATS's intellectual property will be classified as per the Company's data classification policy and labelled and handled as per Company policies.
- Software and hardware will be used in compliance with all legal, statutory, regulatory, and contractual compliance and after due authorization.
- Exception for backup and archival purposes, applicable license, notice or agreement, copyrighted software will not be duplicated.
- The senior manager will be the custodian of the original copies of all Company hardware and software licenses.
- Any software that is acquired illegally or does not have a valid license will not be installed or used on BIM ATS information processing facilities.
- Internal audit team and management team will conduct for the license compliance in last month of every year.
- Employees cannot copy or reproduce in any way, copyrighted material from the Internal on information systems.

13.1.3 Protection of organizational records

BIM ATS management team manages the lifecycle of all records created or received by it in pursuance of legal obligation or transactions of business.

All the company records and information are retained with the retention periods and disposed in secure manner.

13.1.4 Data protection and privacy of personal information

BIM ATS implement controls for collecting, processing, and disseminating personal information. Employee personal data maintained on information systems will be secured through implementation of appropriate security controls. Only limited authorized personnel have access to such information. The security controls will address

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully, and properly.
- Ensuring that information is accurate, complete, and up-to-date, adequate and relevant.
- Appropriate deletion of information.
- Compliance with individual's rights
- Compliance with the relevant data protection/ privacy regulations. BIM ATS management will be responsible for identifying a list of applicable data protection/ privacy regulations and the same will be communicated to the senior manager on a continuous basis
- Contacts with customers handling personal information will include clauses on right to audit.

BIM ATS logs, reviews, and utilizes any personal information stored on or passing through its systems. BIM ATS discrete, monitor usage of the information assets as per applicable laws and terms and condition of employment agreed upon by the company and the employee. This includes logging and reviewing of user activity such as electronic communications exchanged within the Company information processing facilities etc.

13.1.5 Prevention of misuse of information processing facilities

BIM ATS's information system is used only after authorization from management team and for business purpose only. BIM ATS is not responsible for the safe keeping of any personal data on its systems. Employees of BIM ATS assets are not acquired, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, uncles specifically authorized by the management team and IT department.

13.2 Compliance with security policies and standards and technical compliance

13.2.1 Compliance with security policies and standards

Management team prepares an annual plan to ensure its computer and communications systems are compliant with this policy. The senior manager ensures that all security procedures within the area of responsibility are carried out correctly and within the Information Security Management Structure framework. In support of the review, all areas should be considered for regular review to ensure compliance with security policies and standards.

13.2.2 Technical compliance checking

BIM ATS management perform an annual review and random tests of production computer system backup processes. Technical compliance check is carried out regularly, which involves examination of operational systems to ensure that hardware and software controls have been correctly implemented. And as stated in the section 2.3, BIM ATS management team should consider corrective actions.

13.3 Cryptographic controls

13.3.1 Policy on the use of cryptographic controls

- Encryption processes are not set to be used for Company information unless the processes are approved by the senior manager.
- Encryption is adopted for information assets based on the criticality of information as stated in the section 5.2.1. Standard encryption technology would be deployed for encryption unless required by regulatory requirements.
- Users cannot employ encryption, digital signatures, or digital certificates for any business activity or business information without the written authorization of their department manager, the completion of proper training and having their systems configured by authorized personnel.
- Employees cannot employ encryption utilities requiring a user to input a password or encryption key.

14. Non-Compliance

Failure to comply with the Information Security Policy results in disciplinary action by the full discretion of BIM ATS.

-   End of Document -