TAJGVK
TAJGVK Hotels & Resorts Limited

Cyber Consolidated Policies

(As adopted by the Board of Directors on 23.05.2024)

TAJ GVK HOTELS AND RESORTS LIMITED (TAJGVK)

Contents

1. Access Control

1.1 Business Requirement of Access Control

To restrict the access of employees/contractors to information or facilities used for processing the information.

1.1.1 Access Control Policy

- The access to TAJGVK's information and information systems (Operating Systems, Applications, Databases, network equipment and others) should be according to the principles of "least privilege" and "need to know" basis. The procedures should be administered to ensure that the appropriate level of access control is applied to protect the information in each application or system from unauthorized access, modification, disclosure or destruction to ensure that information remains accurate, confidential, and is available when required.
- Where applicable, the policy and procedures may include and abide by the applicable laws.
- In case where customer needs to be provided access to TAJGVK's information or assets, all necessary security requirements shall be identified and addressed before providing any access. All customer access should be approved by the ISM.
- Access control includes enforcement mechanism that operates at three standard levels, facility, system and data.
- Access to information resources shall always be granted in business need, and least privilege principle. The following may be considered by TAJGVK before granting access:
  - Eligibility criteria before granting access.
  - List of facilities, systems, and data to which access needs to be granted.
  - Justification for granting various accesses based on business requirements.
  - Any special instructions from TAJGVK before granting access.
  - All contractual obligations regarding protection of (or access to) data and services.

1.1.2 Access to network and network services

- Employees/contractors may only have privilege to access network for which they are authorized.
- The network services are to be used only for business purpose.
- User authentication shall be required for accessing various networks.
- Monitoring of the network to ensure that the network services are being used for designated purposes.

1.2 User Access Management

The access to system and services should be limited to authorized users whereas unauthorized access to system and services should be prevented or restricted.

1.2.1 User registration and deregistration

- All TAJGVK'S user should be granted access to the information systems and services through a formal user registration process that includes approval of access rights from authorized personnel (Team Lead) before granting access.
- All TAJGVK's user should follow a formal de-registration process for revocation of access to all information systems and services which should include automated or timely intimation and revocation of access rights.
- TAJGVK is recommended to periodically check for removing or blocking redundant user IDs and accounts making sure that they are not issued to other users.

1.2.2 User access provisioning

- A formal process shall be implemented to provide access or revoke access of authorized users to all systems and services.
- TAJGVK shall define and document approval process for providing and revoking the employee/contractor access.
- TAJGVK shall ensure that the level of access granted to users are as per the access policy and is consistence with other requirements such as segregation of duties.

1.2.3 Management of privileged access rights

- Privileges associated with each type of information systems such as Operating System, Business Applications, Databases and Network Elements should be identified and documented.
- Privileges should be allocated to individuals based on authorization from appropriate personnel and based on the requirements of their job function and role,
- Additional privileges more than what is required for the job function may be allowed after getting approval from appropriate personnel from TAJGVK
- Privileges shall be allocated to individuals on a "need-to-use" basis and on an "event-by-event" basis i.e., the minimum requirement for their functional role only when needed.
- TAJGVK shall log the use of privileged user ID and is recommended to review the log periodically.

1.2.4 Management of secret authentication information of users

- TAJGVK is recommended to implement a personal secret authentication information confidential. Users may sign a contract to keep personal authentication information confidential.
- The authentication provided by TAJGVK to employees is recommended to be changed for the first use. TAJGVK may provide authentication parameters in a secure manner.
- The authenticated user ID shall be unique to each employee. Password for authentication is recommended not to be shared with anyone within or outside the organization.

1.2.5 Review of user access rights

- The respective business process heads for all individual users or groups may review the access rights or privileges assigned to the corresponding system periodically.
- Any exceptions noted is recommended to be addressed at the earliest.
- Access rights of employee/contractor on TAJGVK information may be reviewed periodically (say 60 days) to ensure that access provided is appropriate as per job function.
- Employee/contractor activities on information processing facilities is recommended to be logged and reviewed for adherence to security policy.

1.2.6 Removal or adjustment of access rights

- The access of employees or contractors may be removed to their respective information or asset in case of termination from the employment or contract or agreement.
- Access rights for information and information processing facilities may be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors.
- Removal of access rights is suggested to include logical as well as physical access. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights.

1.3 User Responsibilities

Employees/contractors may be guided by TAJGVK not to share organization's information or asset authentication parameters to others. Employee/contractor shall be aware of the contract that is signed by employee/contractor during joining the organization.

1.3.1 Use of secret authentication information

- Employees/contractors may be preferably guided to always follow the TAJGVK's practice to safeguard the authentication information.
- User's responsibility is to not share their secret credentials with other personnel.
- Employee/contractor may preferably avoid keeping record of secret authentication information.
- Secret authentication is suggested not be same and used for business and personal use.
- Employee/contractor is recommended not to use different authentication parameters to use information or facilities within organization.
- Single sign on (SSO) is effective authentication method to reduce the amount of secret authentication information that users need to protect information thus increases the effectiveness of the control.

1.4 System and application access control

Only authorized employees/contractors should have access to system or application. Unauthorized access needs to be restricted.

1.4.1 Information access restriction

- The access of unauthorized personal to information and application should be restricted and it should be as per the organization's access control policy.
- TAJGVK is recommended to provide physical and logical access controls for the isolation of sensitive applications or systems.

1.4.2 Secure log-on procedures

- A secure log-on procedure may be implemented to substantiate the claimed identity of user. Password, smartcards, biometric means are some of the log-on authentication methods by which TAJGVK can secure application or information from unauthorized user.
- The secure log-on procedure is suggested to disclose minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance.
- Any unsuccessful logon attempts may be logged and monitored.
- Minimum Baseline Security Standards may l be developed and maintained.

1.4.3 Password management system

- All User passwords is suggested to be kept confidential and not be shared, posted or otherwise divulged in any manner.
- An initial password may be provided to the users securely during the user creation process and the system should be configured to force the users to change the initial password immediately after the first logon.
- Appropriate procedures may preferably be put in place for storing and management of administrative passwords for critical information systems.
- The following password and account policy may preferably be enforced for all user and administrative accounts on operating systems, applications, databases and all other information protected by password controls:
  - Password's composition= alphanumeric and at least one special character
  - Minimum password length = 8
  - Minimum password age = 7 days
  - Maximum password age = 90 days
  - Password history = 4
  - Inactivity timeout = 10 minutes
  - Account lockout after 5 invalid attempts
- Having a diversified portfolio of applications, mostly specific to hospitality industry, TAJGVK has exempted certain applications to have password policy (to login the application). which that application can support and not matching with the above password policy. However, the access to the application (to run) is recommended to be given through Domain Credentials of the user.

- Deactivation
- Five consecutive invalid login attempts by users will automatically lock or deactivate the user account. In case of logins of privileged accounts, exceptions to lockouts may be documented and approved by the HEAD INFORMATION SECURITY (HEAD - IS).
- Re-activation
- In case of a login account being de-activated, it is recommended that the administrator may reactivate the same on receipt of a request from the user with approval of Team Lead and intimation to Information Security Manager (ISM).
- During odd hours (late night hours / night shifts) it is suggested that, the administrator needs to seek approval from team lead (who in turn will seek consent from the Operation Head over phone. He (the admin) also will respond user mail request stating details of telephonic approval with intimation to Information security Manager. In case where telephonic approval could not be taken (due to unavailability of approving authority), the administrator needs to confirm authenticity of user mail either by speaking to user in person or calling user over phone. After such confirmation the administrator may activate user account and respond the user mail request stating all details with intimation to Team lead /Information Security Manager as applicable.

1.4.4 Use of privileged utility programs

- A proper control is highly suggested to be implemented to restrict the utility programs that might be capable of overriding system and application controls.
- Access to such system utility programs may preferably be regularly monitored reviewed, restricted and tightly controlled. Log shall be maintained for all use of utility program.
- TAJGVK may not be provided its Employees/contractors with utility program that have access to applications or systems where segregation of duties are required.

1.4.5 Access control to program source code

- Access to program source code, designs, and specifications may preferably be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.
- Maintenance and copying of program source library may preferably include strict change control procedure.
- TAJGVK may ensure the integrity in case of publishing the program source code. Appropriate controls and approvals shall be required in order to publish program source code.

1.5 RACI

Activities	Employee/ contractor	Information Security Team	Information Security Manager	Head of IT

Access control policy	I	I	R	A / C
Access to networks and network services	I	R	R / C	A
User registration and de-registration	I	R	R / C	A
User access provisioning		R	R	A
Management of privileged access rights		R	R	A
Management of secret authentication information of users	R		C	A
Review of user access rights		R	R	A / C
Removal or adjustment of access rights	I	R	R / C	A
Use of secret authentication information	R	-	-	-
Information access restriction		R	R / C	A
Secure log-on procedures		R	R / C	A
Password management system	I		R	A
Use of privileged utility programs			R	A
Access control to program source code			R	A / C

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

2 Asset Management

2.1 Important Assets

- Information assets: Databases and data files, contracts and agreements, system documentation, user manuals, training material, operational or support

procedures, business continuity plans, fallback procedures, audit trails, and archived information

- Hardware: e.g., laptops, desktops, servers, routers, firewall printers, but also mobile phones or USB memory sticks and all other network & telephony devices.
- Software: Application software, system software, development tools, and utilities o Infrastructure: e.g., offices, electricity, air conditioning - because those assets can cause lack of availability of information.
- People: People are also considered assets because they also have lots of information in their heads, which is very often not available in other forms.

2.2 Responsibility for Assets

The asset owner is accountable for the comprehensive of protection of information assets. The asset owner may delegate the responsibility of applying the relevant controls for the maintenance of the assets to an individual/ function referred to as the asset custodian. It is the responsibility of the asset custodian to implement appropriate security controls that are required to protect the information assets. It is the responsibility of all employees/users and 3rd parties to maintain confidentiality, integrity and availability of assets that they use. ensure:

- Specifying how the data can be used.
- Identifying those items of data within the area of responsibility
- Agreeing who can access the data and what type of access each user is allowed.
- Determining the sensitivity level of the data.
- Periodically reviewing that sensitivity.
- Approving the security protection procedures for that data.
- Ensuring compliance, where necessary, with the latest Personal Data Protection Act.

2.2.1 Inventory of Assets

- Organizational asset should be identified and their importance is documented. The organizational asset includes information and facilities to process the information.
- The asset information should be maintained in a dedicated inventory. The asset inventory should be up to date, consistence and aligned with other inventories.
- The Information Asset Inventory must contain the following information as a minimum-
  - Asset identification
  - Asset description
  - Asset location
  - Asset Owner/Custodian
  - Asset classification
  - Validity of the classification
- TAJGVK shall ensure that for each of the identified assets, ownership of the asset should be assigned and the classification should be identified.

2.2.2 Ownership of Assets

- TAJGVK shall define an asset owner for each asset. The asset owner shall be responsible for management of the asset.
- The asset owner shall be responsible for the protection of assets/ information processing facilities, controlling the asset and use of asset.
- Asset owner shall periodically review the asset restrictions.
- The asset owner should ensure that o Assets are inventoried o Assets are properly classified o Assets are up to date in the inventory and o Assets are appropriately labelled and handled

2.2.3 Acceptable Use of Assets

- TAJGVK shall define the policy for acceptable use of information assets
- Every Employees/contractor having access to the asset should be well aware of information securities policies of the organization. They shall be responsible for use of information processing facilities and any such use carried out under their responsibility.
- Information resources must not be used for personal benefit, political activity or for the solicitation of performance of any activity that is prohibited by TAJGVK.

2.2.4 Return of Assets

- Employees shall return the assets to the organization in case of termination or transfer.
- TAJGVK shall ensure the protection of asset and control unauthorized copying of relevant information in case of termination of an employee/contractor.

2.3 Information Classification

Information should contain appropriate level of protection according to its importance to the organization. Information should be managed in such a way that it cannot be misused.

2.3.1 Classification of Information

- All organizational asset and information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure. Information and asset classification should be included in the organization's process.
- The level of protection in the classified scheme should be accessed by confidentiality, integrity and availability for the information. Corrective and preventive measures to be taken care for sharing and restricting information.
- Information or asset shall be classified different levels for information-
    - **Restricted**-Information or information processing facilities which are highly confidential and highest value to TAJGVK, only limited and appropriate person shall have access to the information. Few examples of restricted information assets include customers Information, system or application passwords, data file encryption keys, marketing strategy and product plans, corporate finance forecasts, strategic planning documents, merger and acquisition strategies and bids etc.

- **Confidential**- Information which are sensitive within the organization and is intended to use of specified personnel. E.g., reports, account files, audit documents, MIS reports, process manuals, firewall rule base and configuration.
- **Internal-** Information which are not so sensitive and used for internal purpose of TAJGVK. The internal information is only intended to employee/contractor of TAJGVK, it shall not be shared with third parties. e.g., company news letters, staff awareness program documentation or bulletins, inventory lists, internal presentations, form formats, etc.
- **Public**-Information which can be shared with third party and is available for internal as well as external release. E.g., job opening announcements, public bulletins, product and service brochures, advertisements

2.3.2 Labelling of Information

- All classified information and asset should be labelled with a set of procedures adopted by the organization.
- Employees/contractors should be made aware of the labelling process.
- Information assets shall be labelled physically or in electronic format. The labelling shall reflect the classification scheme and labels shall be easily recognizable.
- TAJGVK shall give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media.
- Information classification labels shall appear on all the removable media containing information such as hard copies, floppy disks, CD's etc.

2.3.3 Handling of Assets

- Procedures should be made for handling, processing, storing and communicating information as per their classification scheme.
- Access control to media shall be defined and documented and shall be provided to authorized employee/contractor only.
- Handling of assets include-
  - Storage of asset as per the manufacturer's specification
  - Secure processing
  - Transmission over encrypted connections
  - Disposal of asset/information in ways that they cannot be recovered and reconstituted.

2.3.4 Optimize Asset Costs

All assets should be regularly reviewed to identify ways to optimize costs and maintain alignment with business needs.

2.3.5 Manage Licenses

All software licenses should be managed so that the optimal number of licenses is maintained to support business requirements and the number of licenses owned is sufficient to cover the installed software in use

2.4 Media Handling

To prevent unauthorized access, removal, destruction, unauthorized distribution of information stored in the media.

2.4.1 Management of Removable Media

- Procedures should be made for management of removable media as per their classification scheme.
- A proper encryption technique should be implemented for transmission of confidential data over removable media.
- TAJGVK shall make the contents of re-usable media unrecoverable once it is established that they are no longer required.

2.4.2 Disposal of Media

- Formal procedures to be implemented for secure disposal of media to minimize the risk associated with the information leakage to unauthorized personal.
- The procedure for media disposal should be directly proportional to the sensitivity of the information for the organization.
- TAJGVK shall follow appropriate and adequate controls, background checks and experience of a contractor must be taken into consideration while selecting and assigning them for disposal purposes.

2.4.3 Physical Media Transfer

- Media containing information should be protected against unauthorized access, misuse, corruption during transfer. Proper date, center and transportation system to be maintained for the protection of physical media.
- TAJGVK asset or information shall be protected from loss, damage, misuse or unauthorized access based on the classification level of the information contained.
- TAJGVK must play an active role in identifying and authorizing courier services and ensure reliable medium of packaging and transportation to protect and prevent sensitive information from unauthorized disclosure, modification or any environmental threat.

2.5 RACI

Activities	Employee/ contractor	Asset owner	Department Head	Information security manager
Maintaining Inventory of asset	I	R	A / C	A
Assignment of asset owner	I	I	R / A	I
Acceptable use of assets	R	R / C	A	A

Return of assets	R	R	A / C	I
Classification and labelling	I	R	A	C / I
Handling of asset	R	R / A	A / C	A
Transportation of media	R	A	I /A	A
Disposal of asset	R	R / C	I / A	A
Physical Media transfer	R	R / C	I / C /A	A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

3. Business Continuity Management

A business continuity management process implements to minimize the impact of loss on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.

3.1 Information Security Continuity

The business continuity management process shall include information security requirements of the organization.

3.1.1 Planning information security continuity

- TAJGVK should include information security during planning of business continuity.
- Organization should plan for continuity of information security in case of any disaster.
- TAJGVK shall provide a single point of contact for business continuity to the business area.
- TAJGVK shall provide leadership to the business area for business continuity.
- TAJGVK shall ensure that necessary resources are available in the event of a disruptive event.
- Business continuity of information security shall include-
    - **Business Impact Analysis**- Business impact analysis shall be carried out to identify critical business processes and determine the maximum tolerable period and point of disruption for such critical business processes.

- **Risk Assessment-** Risk assessment shall be carried out to determine potential interruptions, their probability and potential impact of such interruptions, in terms of:
  - time of disruption
  - scale of disruption
  - consequences for information security and
  - Recovery period
- **Identification of business-critical activities-** TAJGVK shall identify the critical activities related to business to ensure continuity of business

3.1.2 Implementing information security continuity

- The organization shall establish, document, implement maintain processes & procedures and controls to ensure the required level of continuity for information security during an adverse situation.
- TAJGVK implement an adequate management structure to respond, mitigate to a disruptive event.
- TAJGVK shall identify the use of resources, services, and fallback procedure to accomplish business objectives.
- TAJGVK shall maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
- TAJGVK shall identify compensating controls to be implemented to mitigate risk due to disaster.

3.1.3 Verify, review and evaluate information security continuity

- The organization should continuously monitor and evaluate the controls of implemented information security continuity in order to ensure that the continuity process is effective in adverse situation or in case of any kind of disaster.
- TAJGVK shall provide copies of business continuity planning (BCP document) to risk management team for review prior to being published on the internet/intranet.
- TAJGVK shall ensure that the business continuity plans are up to date and the performance is consistent with the information security continuity objectives.

3.2 Redundancies

The organization should ensure that the facilities to process the information are available.

3.2.1 Availability of information processing facilities

- Organization shall identify business requirement for the availability of facilities required for the processing of information. Though availabilities cannot be guaranteed, redundant component or architecture should always be considered.
- Redundant information systems shall be tested to ensure the failover from one component to another component work as intended.
- Asset availability is an important part of business and should be available to enable work processes to operate efficiently and effectively.

3.3 RACI

Sr no.	Activities	Information Security Team	Business continuity coordinators	Business continuity manager
1.1.1	Planning information security continuity	I	R	R / A / C
1.1.2	Implementing information security continuity	R	R	R /A
1.1.3	Verify, review and evaluate information security continuity	R / A	R	A
1.2.1	Availability of information processing facilities	R	R / A	R / A / C

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

4. Communication Security

4.1 Network Security Management

TAJGVK should ensure the protection of networks and its supporting information security facilities.

4.1.1 Network Control

- TAJGVK network should be managed and controlled to protect information and system and applications from unauthorized access
- TAJGVK shall implement safeguard measure to maintain confidentiality and integrity of the data processing over the network. It is recommended to have controls in place to maintain the availability of network services.
- TAJGVK shall restrict endpoint access based on the device's compliance with a defined security policy. Offering this form of network security strengthen the security offerings and increase business opportunities.

4.1.2 Security of network services

- TAJGVK shall identify the security measures, service levels and management requirement of all network services and it should be included in network service agreement.
- The organization should provide network in a secure way. The network should be monitored regularly to ensure the protection of data processing over the network.
- TAJGVK shall implement network security measures such as firewalls and intrusion detection systems.

- To maintain the privacy of the TAJGVK information, TAJGVK networks shall not be used for personal and/or private information unrelated to business activities. TAJGVK computers and resources shall be used for valid business purposes only.
- TAJGVK may provide access to third parties after carefully analyzing need and after assessing risks involved in providing such access.
- A legal message may be displayed on the screen whenever a user logs on to the network through any terminal to warn the user on using TAJGVK network for business use only. A message may be displayed on all external network connections warning potential users that unauthorized use is prohibited (e.g. Unauthorized access to TAJGVK network is prohibited).

4.1.3 Segregation in networks

- TAJGVK should segregate network based on based on trust levels (public access domain, desktop domain, server domain) along organizational units (human resource, finance, marketing etc.).
- The perimeter for each domain should be well defined. Access must be controlled using a secure gateway.
- TAJGVK shall implement authentication filtering to restrict access to systems and services based on strong authentication, commonly implemented using cryptography techniques.

4.2 Information Transfer

TAJGVK shall define procedure for the transfer of information over secure network within organization or with any third-party entity.

4.2.1 Information transfer policies and procedures

- TAJGVK shall define and implement policies, procedures and controls to protect the transfer of information using all type of communication facilities.
- Procedures designed shall include the technique to protect transferred information from interruption, modification, copying, destruction and misrouting.
- Cryptographic techniques shall be used to encrypt the confidential information.

4.2.2 Agreements on information transfer

- TAJGVK and the third party shall sign a contractual agreement over the process of information transfer.
- TAJGVK shall be responsible for controlling and notifying transmission, dispatch and receipt of information.
- TAJGVK shall ensure that agreement is covering Information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations specified in compliance policy.

4.2.3 Electronic messaging

- TAJGVK shall protect information involved in electronic messaging.
- TAJGVK shall protect messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by organization.

- TAJGVK shall ensure that all email attachments are scanned with antivirus for all email application.
- Employee shall be aware that, with messages to Internet recipients, he represents TAJGVK publicly.
- It is recommended that stronger level of authentication controls are in place from publicly accessible networks.

4.2.4 Confidential or non-disclosure agreements

- TAJGVK should identify the requirement for confidentiality or non-disclosure agreements reflecting the organization need for the protection of information.
- Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply.
- TAJGVK shall periodically review the confidential and non-disclosure agreements and in case of changes appropriate action shall be taken.

Sr no.	Activities	Employee/ Contractor	Security Team	CISO	Contractor/third Party
1.1.1	Network controls	I	R	R / C / A	
1.1.2	Security of network services		R	R / A	
1.1.3	Segregation in networks	I	R	A / C	
1.2.1	Information transfer policies and procedures	I	R	R / A	
1.2.2	Agreements on information transfer		R	R/ A	
1.2.3	Electronic messaging	R	R	R / C / A	
1.2.4	Confidentiality or non-disclosure agreements			R / A	R / A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

5. Compliance

5.1 Compliance with legal and contractual requirements

Appropriate procedure should be implemented to avoid breaches of legal, statutory or contractual obligations related to information security and other security requirements.

5.1.1 Identification of applicable legislation and contractual requirements

- All relevant statutory, regulatory and contractual requirements, pertaining to the business, shall be defined explicitly and documented for each of TAJGVK's information systems. Where applicable, the policy and procedures shall include and abide by the applicable laws.
- This shall include but not be limited to the IT Act 2000 (Information Technology Act 2000), Companies Act, and Labour Act any other laws or acts applicable to the organization.

5.1.2 Intellectual Property Rights

- The terms and conditions and license requirements of the copyrighted software or any other proprietary information used within TAJGVK shall be complied with.
- TAJGVK shall comply with terms and conditions for software and information obtained from public networks.
- Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material with respect of intellectual property rights, and on the use of proprietary software products.
- TAJGVK shall maintain appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights.
- TAJGVK shall maintain awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them.
- TAJGVK shall provide a policy for maintaining appropriate license conditions and policy for disposing or transferring software to others.
- The proof and evidence of ownership for intellectual property shall be established if and when required.

5.1.3 Protection of Records

- TAJGVK's important records relating to information security shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
- The following areas need to be considered in order to protect TAJGVK's record-
- record categorization, including retention period and storage media;
- storage media deterioration;
- media and format readability;

- Accessibility in a reasonable timeframe;
- Labelling which includes retention period and destruction criteria;

5.1.4 Privacy and protection of personally identifiable information

- Privacy and protection shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses for each business.
- All users shall be made aware about their general and location specific responsibilities to ensure compliance to the applicable data protection and privacy requirements and controls.

5.1.5 Regulation of cryptographic control

• Cryptographic control needs to be implemented in compliance with all relevant agreements, legislation and regulations.

5.2 Information Security Review

• Information should be implemented, operated and continuous monitored according to the TAJGVK policies and procedures.

5.2.1 Independent review of information security

- TAJGVK approach to manage information security and implementation should be reviewed independently.
- Independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.
- Independent review shall identify the TAJGVK's approach to manage information security whether documented objectives and requirements are met.

5.2.2 Compliance with security policies and standards

- Management shall monitor organization information security with appropriate policies and procedures. In case of any non-compliance corrective action shall be taken care.
- TAJGVK shall determine the cause of compliance.
- TAJGVK shall evaluate the need for actions to ensure that non-compliance does not reoccur.
- TAJGVK shall determine and implement appropriate corrective action.

5.2.3 Technical compliance review

- Information processing resources and associated documentation shall be reviewed immediately after installation and thereafter on an annual basis to verify that they are compliant with the security policies and standards. Findings and recommendations in the report shall be communicated to the concerned department personnel for implementation.
- TAJGVK information processing resources shall be reviewed by an independent third-party at least on an annual basis. The findings shall be reported to senior management.

5.3 RACI

Activities	Employee/ contractor	Compliance/ Legal manager	IT/ Information Security manager
Identification of legislation and contractual agreement	I	R / A	C
Intellectual property rights		R / C	A
Protection of records	I	R	
Privacy and protection of personally identifiable information		R / C	A / C
Regulation of control cryptographic		R / A	R
Independent review of information security	I / C	R / A	R
Compliance with security policies and standards		R / C	A / R
Technical compliance review	I / C	A	R

Notes:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

6. Human Resource

6.1 Prior to employment

• TAJGVK shall ensure that employee/contractor shall understand their responsibilities and are suitable for the roles for which they are considered.

6.1.1 Screening Policy

- Background verification checks of all candidates will be carried out at the time of job applications/ after selection.
- Additionally, depending on the sensitivity of the particular job or access level, TAJGVK or an agent appointed by TAJGVK may verify the criminal background of the new employee.
- Such verification checks will be conducted for third-party contractors also.
- TAJGVK shall ensure that employee/contractor is having appropriate competence to fit for the desired role by evaluating employee's CV and conducting interviews.

6.1.2 Terms and conditions of employment

- Every employee joining TAJGVK signs a contractual agreement which state employee and organization's responsibility for information security. It includes-
    - All TAJGVK internal information and,
    - All personal data of TAJGVK employees, TAJGVK customers and TAJGVK contractors he or she has access to.
- The Human Resources department is responsible for managing the signing/ instruction process and retention of the signed confidentiality agreements.
- A signed copy of terms and conditions shall remain with the Human resource team.

6.2 During Employment

TAJGVK shall ensure that employee/contractor is aware of their role and responsibility during employment. TAJGVK shall communicate information security awareness among employee/contractor by conducting training programs, e-learning etc.

6.2.1 Management responsibilities

- Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
- Any change to a user access shall be made in a timely manner and be clearly communicated to user.

6.2.2 Information security awareness, education, and training

- Information Security training and awareness programs shall be provided to all the employees of TAJGVK in order to create awareness about the Information Security policies and processes.
- Information Security Training shall include appropriate training to staff including security breach response responsibilities.
- Department specific information security training would remain the responsibility of the specific department and the operations head.

6.2.3 Disciplinary process

- There shall be a formal and communicated disciplinary process in place to take action against employees who have violated the organization's policy and procedures.
- If a criminal offence is considered to have been committed, further action shall be taken to assist in the prosecution of the offender.
- The formal disciplinary process shall provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence.

6.3 Termination and Change of Employment

• TAJGVK shall ensure the responsibilities of employee/contractor shall remain same after termination or change of employment. TAJGVK shall protect organization's value and interest in case of change or termination of employment.

6.3.1 Termination or change of employment responsibility

- Human resource is responsible for the overall termination process and works together with supervising manager of the contractor/employee.
- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
- TAJGVK shall ensure that employee has returned the assets provided by TAJGVK. Also, access rights to TAJGVK facility shall be removed.

6.4 RACI

Activities	Employee/ contractor	Human resource	Information security manager
Employee/contractor Screening	I	R / A	C
Terms and conditions of employment	R	R / A	-
Management Responsibilities	I	R / A	I
Information security awareness, education and training	R	R / A	C
Disciplinary Process	I	R / A	C / I
Termination or change of employment responsibilities	I	A / R	I

Note:

-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

7. Incident Management

7.1 Management of information security incidents and improvements

A consistent and effective approach or procedure should be implemented to management of information security incidents including communication on security events and weaknesses.

7.1.1 Responsibilities and procedures

- TAJGVK shall establish procedure to identify record, categorize, prioritize and initiate resolution of various types of incidents. TAJGVK shall be responsible for providing quick, effective and orderly response to information security incident.
- TAJGVK shall communicate the procedure to handle/ initiate incident resolution among employee/contractor.
- An incident which causes major disruption of business due to link failure / equipment failure, appropriate Incident Management procedures must be followed.
- TAJGVK shall ensure that in case of incident, management is notified and appropriate action is taken against the incident.
- TAJGVK shall gather physical and electronic evidences as a part of incident investigation. TAJGVK's IT team will be responsible for initiating, completing and documenting the incident investigation.
- Root cause analysis for all reported incidents shall be carried out to identify the underlying cause and prevent recurrence.
- Security incident which cannot be resolved immediately shall be escalated and if required, an effective and accurate work around should be provided in case of any incident.
- TAJGVK shall monitor, analyze and report the information security incident appropriately.
- TAJGVK shall ensure that resolution of incident is accepted by reporting user before closed the incidents tickets.

7.1.2 Reporting information security events

- Information security events should be reported quickly to management.
- Automatic monitoring of systems, alerts, and vulnerabilities shall be used to detect information security events in addition to reporting of incidents.
- All employees/contractors should be made aware of their responsibility to report incident as soon as possible. They should also be aware of process and procedure to report the security incident to management.
- Feedback procedure shall be implemented to ensure that the incident or issues are resolved and closed.

7.1.3 Reporting information security weaknesses

- The employees/contractors should always report the security weaknesses to incident manager (Point of contact) in the information security.
- The reporting mechanism should be quick and easily accessible.
- Appropriate and accessible mechanisms shall be deployed to identify any security weaknesses in TAJGVK information processing systems and services.

7.1.4 Assessment of and decision on information security events

- The incident management team should always review the reported incident. The management needs to classify and prioritize the security event.
- Classification and prioritization of incidents helps the management to find the type and the impact of incident on the business process.
- The management should conduct assessment of information security on regular basis and result of assessment should be kept for future reference. The results lead to avoid reoccurrence of security incidents.

7.1.5 Response to information security incidents

- In case of incident, first response shall be to achieve normal security level and then initiate necessary control or recovery.
- The information security incident should be responded by the incident management team of the organization.
- Incident response activities shall be logged for later analysis.
- Management should review the incident and conduct information security forensics analysis in order to close the incident.

7.1.6 Learning from information security incidents

- The review and result of the resolution of incident should be monitored and saved properly.
- The information gained from evaluation of information security incident should be used to identify the reoccurring of similar incidents. Resolution of previously occurred incidents shall be made available to incident management staff to make use of known errors and workarounds in restoring normal service to the business.
- The incident evaluation report will be helpful in quick resolution of similar incidents in future.

7.1.7 Collection of evidence

- Management should define and apply internal procedure to identify, collect and preserve the information of incident as evidence for disciplinary and legal action.
- Evidence shall be protected from unauthorized access and from modification or damage. Transfers or Copies of Evidence should be approved and witnessed.
- Strong evidence trail should be maintained; this is achieved by bringing about quality and completeness of controls which correctly and consistently protect the evidences.

7.1.8 Major Incidents

- Criteria for categorizing an incident as a 'major' incident shall be defined.
- All major incidents shall have a responsible subject matter expert at all times.
- All major incidents shall be communicated to senior management and relevant stakeholders and resolved on priority.

7.1.9 Employee Responsibilities

- Every employee of TAJGVK owns the responsibility to report security incidents they might be privy or witness to either prior, as they arise or following the incident where it might have been unpreventable at the given time.
- Methods for reporting are as follows: Individuals reporting incidents are required to provide details around the incident including but not limited:
    - Site
    - Incident
    - Date/Time
    - Affected Parties (this might be an individual or a group)
    - Site Management Contact (if known)

7.1.10 Security Incident Management Awareness

• All employees, contractors, subcontractors, agencies, consultants, business partners, visitors. Service providers and third parties will be made aware of the procedures to ensure they are aware of information security threats and concerns encountered in the course of their normal work TAJGVK will develop and make available Security instructor led training and update training as required and notify Business Unit Managers and TAJGVK Relationship Managers of significant updates to the Security Awareness training.

7.2 RACI

Activities	End User	IT Team	Department Head	CMISF
Responsibilities and procedures			R	A / C
Reporting information security events	I	R	R / C	A
Reporting information security weaknesses	R	R	R / C	A
Assessment of and decision on information security events		R	R / C	A
Response to information security incidents		R	R / C	A / C
Learning from information security incidents		R	R / C	R / C
Collection of evidence		R	R / C	A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

8 Mobile Devices and Teleworking

• TAJGVK should ensure the security of teleworking and use of mobile devices.

8.1 Mobile device policy

- TAJGVK shall implement controls to mitigate risk introduced by mobile devices.
- TAJGVK shall adopt a policy and supporting security measures to manage the risks introduced by mobile devices.
- TAJGVK may consider the following parameters for mobile device policy-
    - Registration of mobile devices
    - Requirements for physical protection
    - Restriction of software installation
    - Requirements for mobile device software versions and for applying patches
    - Restriction of connection to information services
    - Access controls
    - Cryptographic techniques
    - Malware protection
    - Remote disabling, erasure or lockout
    - Backups
    - Usage of web services and web apps
- TAJGVK may ensure that care is taken when using mobile devices in public places, meeting rooms and other unprotected areas.
- TAJGVK shall protect mobile devices to avoid the unauthorized access to or disclosure of the information stored and processed by these devices.
- Mobile devices shall be protected physically against theft.

8.2 Use of personally owned mobile devices in TAJGVK environment

All new devices brought in TAJGVK environment accessing TAJGVK's information network shall be submitted to the TAJGVK local IT function for configuration and vulnerability assessment. TAJGVK local IT will decide to configure access to TAJGVK internet on the devices, post verification. For email to be configured on the mobile device or to connect to or access TAJGVK network/ systems through iPad, the user would need to accept the company's acceptable usage policy and e-mail usage policies.

8.2.1 Security Considerations

- TAJGVK shall allow access to company's internet connection only on approved personal devices
- Users shall not be allowed to download any data on the devices. E-mail attachment shall be configured for read only access.

- On-screen passwords shall be mandatory on the devices. Passwords shall be configured as per TAJGVK password policy.
- TAJGVK IT shall implement a technology to logically create a partition in the device. This partition shall segregate user's personal information and applications from official information. Users will not be permitted to access their personal partition in TAJGVK environment. Corporate data will be separated into secure 'containers' and TAJGVK IT shall have full control over them.

8.2.2 Outbound Support Services

TAJGVK will only be responsible for providing email support to the devices under this policy. TAJGVK will not be responsible for providing any other support for hardware or software issues. The employees are expected to use respective device Original Equipment Manufacturer/ application vendors for support, if required.

8.2.3 Ongoing Device Management

TAJGVK shall not be responsible for reimbursing the cost of the user's mobile device/smart phone/laptops, no subsequent costs of maintenance, upgrades or further purchase of accessories will be borne by the company. In events of device being lost, stolen or being rendered useless otherwise, TAJGVK will not be responsible for the replacement of the device or purchase of a new device.

8.2.4 Periodic Audit

TAJGVK IT function may be carry out periodic audits of these devices to identify any exceptions to company policies. TAJGVK IT function may also install MDM solutions on the devices to monitor, manage and secure employees' mobile devices and avoid change of rights imposed by the manufacturer or privilege escalation by rooting or jailbreaking.

8.3 Teleworking

- TAJGVK shall implement policy and security measures to protect information processed or stored at teleworking site.
- TAJGVK may issue a policy that defines the conditions and restrictions for using teleworking.
- Arrangements must be in place to ensure that any TAJGVK teleworking solutions that should be provided are fully supported and maintained.
- Any teleworking equipment which provides remote access to the TAJGVK network, and the authentication method that it uses to access TAJGVK resources, must be approved by the TAJGVK's network team.
- The communications security requirements must be followed, considering the need for remote access to the organizations internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system.

- TAJGVK may implement preventive measures from the threat of unauthorized access to information or resources from other persons using the accommodation, e.g., family and friends.
- TAJGVK shall ensure malware protection and firewall requirements.
- TAJGVK should ensure the software licensing agreements are in such a way that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users.

8.4 RACI

Activities	Employee/ Contractor	IT/Security Team	CMISF
Mobile device policy	R	R / C	A / C
Teleworking	R / I	R / C	A / C

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

9. Operation Security

9.1 Operating procedures and responsibility

TAJGVK should ensure that all the operations related to information security and facilities to process information security should be secure and correct.

9.1.1 Documented Operating Procedures

- Operating procedures for all processes of TAJGVK shall be developed, maintained and published to enable the authorized users, network and system administrators to perform their daily operations.
- Where applicable, the policy and procedures shall include and abide by the applicable laws.
- TAJGVK shall ensure that documented operating procedures are associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

9.1.2 Change Management

- Changes to IT assets (including applications, servers, systems software, and security architecture and network devices) shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. This involves obtaining prior approval, performing impact analysis, testing, and maintaining up-to-date documentation for the entire process.

- Changes shall be tested in a non-production environment before deployment and ineffective changes shall be rolled-back.
- Appropriate procedures shall be put in place for all changes requiring emergency actions and response process, which bypass the policies and procedures outlined.

9.1.3 Capacity Management

• TAJGVK shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of TAJGVK. Where applicable, the policy and procedures shall include and abide by the applicable laws.

9.1.4 Separation of development, testing and operational environments

- TAJGVK should have separate environments for different life cycle of the project. Different and secure environment is required for development, testing and operations respectively.
- There shall be a procedure defined to transfer the software from development stage to testing and operational stage.
- TAJGVK shall provide access to users based on the environment. User's having access to development and testing instance, should not have access to production instance unless authorized for specific business use.
- TAJGVK shall logically and physically separate development, test and production instance to reduce the risk of unauthorized changes to production system.

9.2 Protection from malware

TAJGVK shall have all the preventive measures for malware. Organization should always monitor the information security information and facilities to process information to ensure that systems/software are protected from malware.

9.2.1 Controls against malware

- TAJGVK shall implement the procedure to identify or detect the malware attack and controls needs to implemented to mitigate the risk occurred due to malware
- TAJGVK shall implement a policy which should be secure and shall implement control for protection of facilities and security information from malware.
- TAJGVK shall always have recovery plan in case any malware detection. A necessary action should be taken care to ensure the information is protected.
- TAJGVK must verify that the systems generate an alert or e-mail notice regarding the malware within a certain specified time by TAJGVK.
- Continuous monitoring shall be performed on all inbound and outbound traffic.
- TAJGVK shall configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

9.3 Backup

• TAJGVK shall have backup plan against loss of data.

9.3.1 Information Back-up

- All application and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information, software and log files (logs from various systems that need to be backed) essential to the continued operations of TAJGVK shall be identified, documented and periodically backed up.
- Where applicable, the policy and procedures shall include and abide by the applicable laws.
- Frequency of backup, medium of backup and storage of the backup shall be identified and documented based on the contractual requirements.
- The security controls over the backup of information and media shall be commensurate with the classification of the information backed up, contractual obligations and other applicable guidelines. Back up shall be retained in accordance with the requirements set out in the contractual obligations. Backup register shall be maintained by personnel who take back-up and shall be updated regularly.
- In addition to the scheduled backups, backups shall be taken in case any of the following event occurs:
    - Configuration changes
    - Changes in Operating systems
- Both onsite and offsite backup shall be stored in safe custody in a fire-proof safe. If fire-proof safe is not available, alternate controls shall be put in place to protect those tapes from fire.
- All movement of tapes between offsite and onsite locations shall be tracked and recorded.

9.4 Logging and monitoring

• TAJGVK shall ensure that all the activities of users as well as system related to information security should be recorded or tacked and that should be used as evidence.

9.4.1 Event Logging

- TAJGVK shall be tracking user activities, faults, and authorization, exception and information security events. Based on that an event log shall be prepared.
- The prepared log shall be regularly updated, reviewed and kept protected from unauthorized access.
- TAJGVK shall log and independently review the high-level access of users (such as system administrator access to highly confidentiality information).

9.4.2 Protection of log information

- TAJGVK should have controls to protect against tempering and unauthorized access to log information and operational problems.

- Log information may contain highly confidential data and personal identifiable information, TAJGVK shall provide high level protection to log file and shall be stored in secure manner.
- If the log file has exceeded the capacity, it should be achieved and protected from unauthorized personal.

9.4.3 Administrator and operator log

• Administrator and operator activities log shall be separately reviewed and the log shall be protected from unauthorized access.

9.4.4 Clock Synchronization

- TAJGVK shall maintain and synchronize clocks of all relevant information security processing facilities with the organization.
- The clocks of all relevant information processing systems within TAJGVK or security domain shall be synchronized with an agreed accurate time source.
- The correct setting of computer clocks is important to ensure the accuracy of audit logs, which is required as evidence in legal and disciplinary case.

9.5 Control of operational software

• TAJGVK shall implement controls for operational systems to maintain the integrity.

9.5.1 Installation of software of operational systems

- TAJGVK should implement a procedure to install or update software or application to operational system, the software should be licensed, virus free and protected.
- Impact analysis shall be done before update or installing software to operational system. Proper documentation is required to analyze the impact.

9.6 Technical vulnerability management

TAJGVK shall prevent exploitation of technical vulnerabilities.

9.6.1 Management of technical vulnerabilities

- TAJGVK shall review information system and obtain information about technical vulnerabilities in timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
- Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment and the person[s] within the organization responsible for the software.
- In case of technical vulnerability, TAJGVK shall identify the risk associated with the vulnerability attack and appropriate action shall be taken care to reduce the risk.

9.6.2 Restrictions on software installation

- TAJGVK shall define and document rules for the installation of software by users.

- TAJGVK should ensure which type of software should be installed and who is authorized to do the operation.
- Only licensed version of software shall be installed in the TAJGVK's system. Unauthorized and uncontrolled devices lead to loss of data, misuse and loss of integrity.

9.7 Information systems audit considerations

Impact of audit activities shall be minimized by proper planning of business process.

9.7.1 Information system audit controls

- Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruption to business processes.
- The scope of technical audit should be well documented and should be limited to authorized access.

9.8 RACI

Activities	Employee/ contractor	Operations Team	Security / IT Team	Operations Head
Documented operating procedures		R	R	C / A
Change management	I	C	R	A
Capacity management		R		A
Separation of development, testing and operational environments		R		A
Controls against malware		R / C	R	A
Information back and		R / C	R	A
logging				
Protection of log and information document	R	R / C	R	A
Administrator and operator logs		R		R / A
Clock synchronisation		R / C	R	A
Installation of softwar operational systems	I	C	R	A
Management of technical vulnerabilities		R	R	A / C

Restriction on software installation	I / R	C / A	R	A
Information systems audit controls		R		A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

10. Physical and Environmental Control

10.1 Secure Areas

TAJGVK should have a procedure to prevent unauthorized physical access, damage and interference to organization's information and system.

10.1.1 Physical Security Perimeter

- Physical protection can be achieved by creating several physical barriers around the building premises and information processing facilities.
- Each barrier establishes a security perimeter increasing the total physical protection provided. A security perimeter can be a wall, a card-controlled entry gate or a manned reception desk.
- The TAJGVK offices shall be logically divided into different zones. Each zone shall have appropriate level of access restrictions and access authorization requirements.
- Areas containing critical IT equipment (such as the Hub room and the data centers) shall be designated as high security zones. Where applicable, the policies and procedure shall include and abide by the applicable laws.
- All the Firefighting equipment, fire alarms should be monitored and tested in conjunction with required level of resistance.

10.1.2 Physical Entry Controls

- Only those employees, whose job description demands access to TAJGVK's Systems, shall be allowed to enter the premises.
- Visitors' entry into the premises shall be restricted by appropriate security validations like checking the identity of the visitor, random frisking, checking their belongings and bags, etc.
- There shall be 24 x 7 guarding of premises by a designated security agency.
- The credentials of the security personnel posted at such premises shall be verified with the agency to mitigate risks of theft or vandalism. The contact information of the security agency shall be maintained by the TAJGVK Administration Department for easy identification in the eventuality of a mishap.
- All movement of material going in and out of premises shall be duly authorized and tracked.
- Access rights to the secure areas shall be regularly reviewed, updated and revoked when necessary.

10.1.3 Securing offices, room and facilities

Depending on the sensitivity of information handled within, the physical security for offices, rooms and facilities shall be designed and applied. Access to hub room shall be restricted. Only the Networks team personnel and those authorized shall be allowed to access the Hub room.

10.1.4 Protecting against External and Environmental threats

- TAJGVK's offices shall be fitted with appropriate firefighting devices at critical locations in order to arrest the fire and to avoid damage to the various resources of TAJGVK. Safety measures like fire and earthquake evacuation drills shall be practiced regularly.
- Appropriate safety measure shall be taken to avoid loss and damage due to water flooding or inappropriate drainage system within the premises of TAJGVK.
- Physical protection against damage from natural or man-made disaster shall be designed and applied.
- Back-up media should be distant from a disaster affecting the main site and combustible materials should be distant from secure areas.

10.1.5 Working in Secure areas

- Physical protection and guidelines for working in secure areas shall be defined and applied. Third party support service personnel shall be granted restricted access to secure areas.
- Photographic, video, audio or any such recording equipment should be prohibited unless authorized
- Vacant secure areas should be physically locked and monitored regularly.
- The access shall be authorized and monitored.

10.1.6 Delivery and loading areas

- Access points such as delivery areas and other points where unauthorized personnel may enter the premises shall be controlled and isolated form information processing facilities.
- Incoming material should be inspected for potential threats before moving it to the point of use.

10.2 Equipment

TAJGVK should take all the preventive measure to control loss, damage, theft or compromises of assets and interruption to organization's process or operations.

10.2.1 Equipment sitting and protection

- All electronic office equipment including faxes, printers, photocopiers etc., shall be physically secured.
- Security of Desktops and Network hubs
    - Desktops shall be adequately protected from fire, water and pollution damage and power supply fluctuations.
    - Networks hubs shall be secured from fire, heat, dust and water
    - Interception or damage to Network cables shall be controlled.
- Media handling and security
    - Media shall be protected from physical damages like fire, moisture and magnetic interference
    - A stock or inventory of all the media shall be maintained

- Media shall be disposed off securely and safely when no longer required. Formal procedures for the secure disposal of media shall be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

10.2.2 Supporting Utilities

- Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications.
- Options to achieve continuity of power supplies include:
  - Multiple feeds to avoid a single point of failure in the power supply
  - Uninterruptible power supply (UPS)
  - Back-up generator
- A UPS to support orderly close down or continuous running shall be implemented for equipment supporting critical business operations. Contingency plans shall cover the action to be taken on failure of the UPS. UPS equipment shall be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.
- A back-up generator shall be considered if processing is to continue in case of a prolonged power failure. If installed, generators shall be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period.
- In addition, emergency power switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting shall be provided in case of main power failure. Lightning protection shall be applied to all buildings and lightning protection filters shall be fitted to all external communications lines.

10.2.3 Cabling Security

- Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
- TAJGVK shall ensure that power and telecommunication cables are underground, where possible, or subject to adequate alternative protection.

10.2.4 Equipment Maintenance

- TAJGVK shall implement appropriate controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization
- Equipment shall be maintained to ensure its availability and integrity.

10.2.5 Removal of Asset

- Equipment, information or software shall not be taken off-site without prior authorization.
- The following controls shall be applied:
  - Employees, third-party and contractors who have the authority to take the equipment off-site shall be clearly identified.

- Time limits for equipment removal shall be set and returns checked for compliance.
- Equipment shall be recorded as being removed off-site and recorded when returned.

10.2.6 Security of equipment and asset off-premises

- Security shall be applied to off-site asset (e.g. Laptops, Servers etc.) taking into account the different risks of working outside the organization's premises.
- TAJGVK shall maintain a log which includes the name and organization of individuals who are responsible for the equipment when it off-premises.

10.2.7 Secure disposal or Re-use of equipment

- TAJGVK shall verify the equipment to ensure whether it contains important information and a backup is stored for further use.
- IT hardware and equipment shall be disposed off only after approval. Further, data and media destruction shall be performed prior to disposal of equipment.
- Disposal of retired hardware and media shall comply with prevalent environmental regulations.

10.2.8 Unattended user equipment

- TAJGVK shall ensure that unattended computing equipment has appropriate protection.
- All employees/contractors should be made aware of security requirements and procedures to protect unattended equipment.

10.2.9 Clear desk and clear screen policy

- All document related to information security of the organization should be kept confidential and locked.
- Applications/systems containing information should be logged off after use.
- Any information security related document should not be kept at desk to avoid any kind of risk and loss.
- Employee/contractor shall not write down user name and password on computer or desk.
- Employee/contractor shall not leave laptop/desktop unlocked when it is not in use.

10.3 RACI

Activities	Employees/ contractors	Media handling/ security team	Infrastructure/ Facility Team	CMISF/ PMISF
Physical security perimeter	I	C	R	A

Physical entry controls	I	C	R	A
Securing offices, rooms and facilities	I	C	R	A / C
Protecting against external and environmental threats	I	C	R	A/C
Working in secure areas	R	R	R	A
Delivery and loading areas		R	R /C	A
Equipment siting and protection	I	R	R / C	A
Supporting utilities	R	R	R	A
Cabling security	I	R	R	A
Equipment maintenance			R	A
Removal of assets	R	R	R	A
Security of equipment and assets off-premises	R	R	R	A
Secure disposal or re-use of equipment		R	C	A
Unattended user equipment	R	R	R	A
Clear desk and clear screen policy	R	R	R	R / A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

11. Cloud Security

11.1 Overview

The number of Cloud service providers and Cloud-based solutions has considerably increased in recent years. This wide variety of solutions and the potential threats, vulnerabilities and resulting risks, have led TAJGVK to define this policy. The most important classes of Cloud-specific security risks are:

- Loss of governance
- Vendor lock-In
- Isolation failure
- Non-compliance
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

Since Cloud-based solutions store "business data" outside of the Group which may be legally confidential and/or restricted to be made public, information security requirements must be ensured to protect the confidentiality, integrity and availability of data.

This policy defines the security requirements for using the authorized Cloud-based solutions

11.2 Purpose

This policy constitutes a practical guide to address security in a Cloud computing project, which fully complies with the Information Security Policy rules in terms of the required level of security, e.g., confidentiality, integrity and availability for TAJGVK's data and applications.

11.3 Definition

Term	Definition
Public Cloud	The Public Cloud is the computing service provided by the cloud providers over the public Internet. The applications hosted on the cloud will be accessible to any one over the cloud.
Private Cloud	The Private Cloud is the computing service provided by the cloud providers over the Internet or a private internal network. The applications or services running over the cloud is accessible by only few selected users.
Hybrid Cloud	A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

Cloud Software as a Service (SaaS)	Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet. The organization borrows the application for the users. All the underlying infrastructure, middleware, app software and app data are in the service provider's data centre.
Cloud Platform as a Service (PaaS)	Platform as a service (PaaS) is a complete development and deployment environment in the cloud, which enables to host applications or services without worrying about infrastructure (servers, storage and networking), middleware, development tools, business intelligence services and database management systems.
Infrastructure as a Service (IaaS)	Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet. A cloud computing service provider manages the infrastructure, while the organization purchase, install, configure, and manage the software—operating systems, middleware, and applications.

11.4 Scope

This policy presents the rules that must be followed by TAJGVK in all entities when dealing with Cloud-based solution. This policy applies at all stages of the lifetime of a Cloud-based solution (e.g., pre-study / short listing, implementation project and maintenance period). This policy does not apply to TAJGVK "Internal Cloud" solutions.

TAJGVK, through CISO should ensure that all requirements are implemented. Applicable recommendations should also be considered for implementation.

11.5 Policy

TAJGVK, through CISO, should ensure that all requirements are implemented. Applicable recommendations should also be considered for implementation.

11.5.1 Priority Requirements

C#	Control statement	Requirement/ Recommendation
# 1	All new Cloud services must be reported to and validated by CISO/IT team.	Requirement
# 2	The use of any unapproved Cloud services for the storage or transmission of corporate information must be forbidden.	Requirement
# 3	Cloud services shall comply with all applicable IT Security policies and procedures of TAJGVK.	Requirement

#4	In case of a new Cloud related initiatives, the CISO shall ensure that Project Owner and other relevant actors follow the defined TAJGVK Supplier Relationships Procedure	Requirement
# 5	In case of a new Cloud related initiatives, the CISO shall ensure that all requirements detailed in the present Cloud Security Policy (see below "5.2.2 Risk management" to "5.2.11 Legal framework") shall be applied.	Requirement
# 6	In case of a new Cloud related initiatives, the CISO must carry out a risk assessment. The risk assessment must consider Cloud-specific risk scenarios, such as: • Data Protection in an environment with shared Responsibilities • Loss of governance as controls are partially ceded to the cloud provider • Vendor lock-in • Isolation failure in a multi-tenant infrastructure • Management interface compromise • Insecure or incomplete data deletion • State sponsored espionage	Requirement
# 7	In case of hosting sensitive data as defined according to TAJGVK Asset management procedure in Cloud services, strong authentication (e.g., Multifactor Authentication) shall be applied to conduct access control for employees and partners.	Requirement

# 8	Cloud management interface used for IT Administrators should be protected by strong authentication (e.g., Multi-Factor Authentication) and administrative operations may be logged. Delegated administration using roles must be implemented to divide technical operations based on the respective scope of the administrators (level of responsibility, geographical scope, and division scope).	Requirement

# 9	Cloud-hosted applications must be included in the scope of the IT vulnerability assessment / penetration testing program and be tested as defined in TAJGVK operations security procedures and at least on a yearly basis. The assessment conclusions must be communicated to CISO/IT team. The following components must be considered in the scope of the assessment: • Cloud-based operating systems and databases; • Cloud networking infrastructure; • Cloud-based applications; • Cloud-based management and monitoring system; • API/Webservices, needed for integration/interface with existing systems	Requirement
# 10	Communications between the Cloud provider and TAJGVK internal network should be through secure channels (e.g., encryption). The protection level shall be based on the assessment of the data sensitivity.	Requirement
# 11	CISO, in consultation with Legal, shall ensure a data security breach notification procedure is defined with Cloud provider to determine the necessary course of actions to follow if data breach is detected. Notification to the individuals possibly concerned by the breach should be considered.	Requirement
# 12	Security monitoring of Cloud-based applications and services shall be integrated with the SIEM tool used for TAJGVK Security Monitoring. Audit logs must be shared as in when demanded. The recommendations of Security Operation Centre shall be implemented by cloud service provider	Requirement

11.5.2 All Requirements and Recommendations

11.5.2.1 New Cloud Services

- In case of a new Cloud related initiatives, the CISO shall ensure that all requirements detailed in the present Cloud Security Policy (see below "5.2.2 Risk management" to "5.2.11 Legal framework") shall be applied
- All new Cloud services must be validated by IT team/CIO and approved by CISO.
- The use of any unapproved Cloud services for the storage or transmission of corporate information must be forbidden or highlighted to Board.
- Cloud services shall comply with all applicable IT Security policies and procedures of TAJGVK.

- In case of a new Cloud related initiatives, the CISO shall ensure that Project Owner and other relevant actors follow the defined TAJGVK Vendor Management Security Policy.
- Contingency plans need to be created to handle possible disaster situations if there were issues with the cloud provider. Scenarios within the plan should include the following: What if the cloud provider goes offline or go out of business or stop offering cloud service?

11.5.2.2 Risk Management

- In case of a new Cloud related initiatives, the CISO must carry out a risk assessment. The risk assessment must consider Cloud-specific risk scenarios, such as:
    - Data Protection in an environment with shared responsibilities
    - Loss of governance as controls are partially ceded to the Cloud provider
    - Vendor lock-in
    - Isolation failure in a multi-tenant infrastructure
    - Management interface compromise
    - Insecure or incomplete data deletion
    - State sponsored espionage
    - Cyber Security incident
- The cloud provider must review the risk management of their partners so that practices are consistent and aligned.
- As part of the risk assessment, the Cloud service provider shall be evaluated to determine if it can be a trusted provider for TAJGVK.

11.5.2.3 Data Protection

- Data hosted in a Cloud service must be classified based on the results of risk assessment.
- CISO shall ensure that relevant data protection measures are implemented according to the data classification and risk assessment results (encryption at rest or transported across the network for sensitive data, etc.).
- Due to the use of mutualized resources, data destruction procedures must use secure deletion methods such as crypto-shredding, disk wiping and other related techniques.
- The cloud provider must retain the data as per the customer data retention policy and provide physical location/ geography of the datacenter.
- Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return all [term for sensitive data] to Institution or, if return is not feasible, destroy all data with a confirmation certificate issued to TAJGVK

11.5.2.4 Data Privacy

- TAJGVK must verify the lawfulness of hosting PII in the regions used to host the application or service and keep track of these geographies.
- TAJGVK, through service provider, must comply with standards regarding privacy, as listed in various laws (e.g. GDPR, CCPA. PCI etc.)

11.5.2.5 Access Control

- Access control level shall be adapted for customers to the results of risk assessment and business requirements.
- In case of hosting sensitive data as defined according to TAJGVK Asset Management Procedure or PII in Cloud services, strong authentication (e.g., Multi-Factor Authentication) shall be applied to conduct access control for employees and partners.
- The cloud provider must provide with local authentication through IDAM, solution integrated with customer's IDAM solution or SSO (Single Sign-On).
- Cloud management interface used by IT Team should be protected by strong authentication (e.g., Multi-Factor Authentication) and administrative operations shall be logged.
- Delegated administration using roles must be implemented to divide technical operations based on the respective scope of the administrators (level of responsibility, geographical scope, and division scope) and employees. Timely de-provision, revoke or modification of roles must be done in case of change of role of user.
- The cloud provider must have controls to remove access rights and permissions which are no longer required.
- The cloud provider must document, if required, access of customer's trust sources such as ADFS. The document must also include policies and procedures secure the same. If ADFS integration is not in place, the cloud provider must provide provision to set password policy and centralized managed.
- The Cloud provider must have the functionality of classifying provider and customer data. The access to the data must be restricted with access policies.
- Cloud provider must have provision to provide access to logs of information security management systems

11.5.2.6 Application Security

- Cloud-hosted applications must be included in the scope of the IT vulnerability assessment / penetration testing program and be tested as defined in TAJGVK Operations security procedure and at least on a yearly basis. The assessment conclusions must be communicated to CISO/IT team. The following components must be considered in the scope of the assessment:
    - Cloud-based operating systems and databases;
    - Cloud networking infrastructure;
    - Cloud-based applications;
    - Cloud-based management and monitoring system.
- The perimeter security mechanism provided by the cloud provider must protect against:
    - Authentication related attacks
    - Session related attacks
    - Injection related attacks
    - Unvalidated Redirects and Forwards attacks

- Database related attacks
- Function Level Access Control related attacks
- Fuzzing attacks

- The IT vulnerability assessment/testing program must cover all of the below:
  - Vulnerability scans;
  - Penetration testing
  - Configuration review.

The assessment report must be shared with the customer.

- Non-production environments (e.g., development, testing, QA, pre-prod) must be segregated from the production environment:
  - environments must reside in different virtual networks;
  - firewall rules must restrict access to each network.
  - Production environment data must not be replicated or used in non-production environment.
- Test user access to non-production environment should be protected using either:
  - IP whitelisting;
  - Password protection;
  - Access possible only through TAJGVK internal network.

11.5.2.7 Infrastructure Security

- Communications between the Cloud provider and TAJGVK internal network should be through secure channels (e.g., encryption). The protection level shall be based on the assessment of the data sensitivity.
- The cloud service provider must have provision to define customer acceptable geographical locations for data routing or resource instantiation.
- The cloud provider must have provision to meet the customers' availability requirements.
- The cloud provider must provide provision to utilize synchronized time-service protocol with proper authentication (ex. NTP) to ensure all systems have a common time reference.
- IT team shall account for availability requirements and develop a Business Continuity Plan / Disaster Recovery Plan which is tested on a regular basis (including the granularity of the restoration process, the restore point objective, restore time objective and minimum acceptable recovery configuration).
- Based on the risk assessment of the project, additional perimeter security mechanisms should be considered such as:
  - Next-gen firewall;
  - Web application firewall;
  - IDS/ IPS.
  - Secure Web Gateway
  - Multi anti-malware

- Cloud service provider must provide adequate security to block unauthorized access to system, theft or destruction of data, hacker attacks, denial of service attacks, and malicious code.
- The cloud service provider must provide details of network firewall (make and model) and firmware version deployed to the customers.
- Cloud provider should follow cloud security, information security and structured data labelling standard e.g., BS25999, ISO 22301, ISO 27001, ISO 15489, CSA data type guidance, GIA and must be certified by third party vendors for the same. The certifications must be shared with the customers.

- Cloud service provider must share document stating the roles / rights / responsibilities of the customer at the time of production change.

11.5.2.8 Operations Security

- Backup procedures must be compliant with TAJGVK standards. Backup data must be stored in a different hosting geography from the main production environment. Sensitive data or PII must be encrypted within backup or the full backup must be encrypted.
- The Cloud service must have the provision of restoring the computing services (Virtual machines, Container and serverless) to the previous stable state. Also, customers must be allowed to download the images of computing services and be able to run on other cloud provider computing services.
- The cloud provider must have provision of maintaining logs of any changes made in the resources and to notify the concern for any such activity.
- The cloud provider must share information system document (e.g., administrator and user guides, architecture diagrams, etc.) for proper configuring, installing, and operating of the information system.
- CISO shall ensure a TAJGVK Information Security Incident Management Procedure is defined with Cloud provider to determine the necessary course of actions to follow if data breach is detected. Notification to the individuals possibly concerned by the breach should be considered.

11.5.2.9 Security Patch Management

SaaS Solution

- The contract entered with each SaaS vendor should include relevant clauses that ensure the vendor continually applies security patches to their underlying infrastructure firmware and software, hypervisors, operating systems and applications in a timely manner that ensures such patches are applied within the following maximum timeframes:
    - Out of band emergency patches - 7 days
    - Critical and High-risk security patches - 15 days
- The risk level shall be assessed and declared by the hardware/software vendor and will be used as the referential

Non–SaaS Solution

- For non-SaaS solutions, both the Cloud provider, TAJGVK IT team and third-party support organization contracted to operate the platform on behalf of TAJGVK IT team take on some level of joint responsibility for maintaining the overall environment. No matter what the breakdown in responsibility the outcomes must be as follows:
    - Cloud provider must be contractually bound and ensure they apply all released and relevant security patches for the portion of the environment they are responsible for within the maximum timeframes listed within the SaaS section.

- TAJGVK IT team or third-party support organization shall ensure all released and relevant security patches for all remaining parts of the environment that fall outside the scope of the Cloud provider.

11.5.2.10 Log Management and Auditing

- All actions performed by the vendor's personnel must be logged and reviewed in relation to their access to the platform and solution environment.
- All security alerts generated for the web application server must be monitored, logged for further analysis and be notified to the concern person. The reports of the any information security incident must be shared with the customer.
- The logging and monitoring framework deployed by the cloud provider must be able to isolate incidents to specific customers.
- Security monitoring of Cloud-based applications and services shall be integrated by the security monitoring solutions integrated with TAJGVK Security Monitoring. Audit logs must be shared as in when demanded.
- Audit log of the management console must be reviewed on a defined basis to detect any non-compliant operation. The log must be shared to the concerned person.
- TAJGVK should audit the vendor's security or at least have access to third party audits that have been conducted at least on an annual basis by a known and reputable third-party organization not affiliated with the vendor.

11.5.2.11 Legal Framework

- The contract must include a clause describing the risk assessment conclusions performed on the application or service that would be outsourced. The Cloud service provider shall engage to address the risk assessment conclusions (see 5.2.2 Risk management).
- The contract must define the property of the data. TAJGVK must keep the property of all sensitive data.
- The contract must define the portability of the application and data for sensitive applications.
- The cloud provider must provide with structured and unstructured data, as per customer request, in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and files).
- The contract must define that business data stored at a Cloud service provider shall remain available even if the contractual relationship with the Cloud service provider be terminated by either party.
- The contract must define a clause for reversing. It should include information on:
  - Operations to recover all the data;
  - technical documentation for data reuse;
  - Operations to securely erase data in case of termination of the contract or as a result of a legal or statutory compliance requirement.
- Formalized contracts, NDA and Service Level Agreements (SLAs) must be agreed between TAJGVK and the Cloud service providers. Roles and responsibilities and

key Service Level Objectives shall be agreed and documented in the contracts and SLAs.

- Vendor should provide a security incident response plan that is reviewed and accepted by TAJGVK, which needs to be in accordance with the TAJGVK Information Security Incident Response Policy. It shall be contractually obligated to notify TAJGVK in the event of a security incident that did or may impact TAJGVK.
- The contract must define a clause ensuring that in case of a major security alert, the patch would be deployed on the machine hosting the application according to 5.2.9 Security patch management.
- The contract must define an audit clause allowing TAJGVK to make or mandate an audit on critical security points in the service or to get the results of such audits performed by third party. The audit minimal frequency should be once a year.
- The contract must define a declaration of compliance with all applicable rules and laws. TAJGVK should not be responsible if no compliance problems occurred with software or hardware licenses.
- The contract must define the responsibility of the provider and how TAJGVK can control that the provider respects its commitments if the application is submitted to specific regulations. A particular attention should be made for application handling no public personal data.
- The contract must define a clause to ensure that legal requests can be processed by the Cloud service provider.
- Vendor must provide written assurance that they have a robust process in place for vetting all their personnel and employee backgrounds.
- All subcontractors must be bound by the same security requirements as followed by the vendor.
- Contract with a cloud provider should have provisions around what happens with your data in the event of bankruptcy, default, service changes, etc
- The contract must define a penalty clause permitting TAJGVK to get a financial compensation in case of default of the provider. The penalties shall be compared with the potential lost seen at the risk assessment step.
- The TAJGVK CISO must be involved in the contract defining and reviewing process.
- Any applicable requirement verified during the Cloud provider evaluation procedure, shall be adapted as a clause integrated in the contract (e.g., vulnerability scan).
- A document must be defined stating the non-disclosure and confidentiality agreements of the organization's operational details and data. The document must be reviewed at planned intervals.

11.5.2.12 Data Centre Security

- Cloud provider must provide documentation to the customers, stating a list of scenarios where data be moved from one physical location to another.

- Cloud provider must provide policies and procedures governing asset management and repurposing of equipment.
- Cloud provider must share documents on the segregation of duties within the cloud services.

11.6 Auditing

- An audit plan must be elaborated on periodic basis, driven by a risk assessment process performed by independent auditors and accepted by the management.
- The audit plan covers the assessment based on test of design and effectiveness of the Information Security Management System (ISMS) and the implemented security controls in selected areas within TAJGVK.

11.7 Performance and reporting

- The IT security exposure, risks, performance and incidents must be reported on a regular basis to Senior management and CISO, considering internal and external factors.
- Based on these reports, CISO and IT team is responsible to take corrective actions where required and provides resources and budget for the same.

11.8 Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Ensuring overall compliance with the present policy • Ensuring each new Cloud initiatives follows the defined TAJGVK Supplier Relationships Procedure and requirements defined in this policy • Providing support for risk assessment, recommendations and Implementation of appropriate controls • Involved in the contract defining and reviewing process
TAJGVK IT team	• Developing the Business Continuity Plan / Disaster Recovery Plan based on the availability requirements • Implementation of necessary security measure to comply with the security requirements defined in the present policy

11.9 Compliance and Enforcement

Periodic audits of compliance shall be conducted at least annually. Results shall be documented, and any deficiencies corrected.

11.10 Exception

Any exception to this policy must be documented and forwarded to the Chief Information Security Officer CISO for review and approbation, which needs to be vetted by CIO also.

11.11 Monitoring and Reporting

This document shall be reviewed once a year or at the time of any major change in existing environment affecting policy, whichever is earlier.

This document contains controlled copies of the procedure listed above. Any copies made from this document, in part or in whole, are uncontrolled and are therefore not subject to further review, revision or approval.

12 Social Media

- Employees/contractors shall ensure that they are aware of use of social media policy to include blogs, microblogs, wikis, message boards, chat room, social networking sites and services that permit users to share information and personal details with others.
- TAJGVK shall keep track of what employees/ contractors are posting or twitting about especially on the issues that pertain to the workspace.
- TAJGVK's employees shall be restricted to publish or comment via social media in accordance with this policy.

12.1 Employee responsibility

- Employee/contractor shall know and adhere to the company code of conduct or policy when using social media.
- Social media sites shall be used only for authorized business purpose through corporate network after prior approval.

12.1.1 Setting up social media

- It is highly recommended that employees keep professional social media accounts (e.g. LinkedIn) separate from personal accounts, if practical.
- Employees/contractors shall always use strong password for authentication to social media. The password shall not match with TAJGVK's user ID.
- Employee/contractor shall be transparent. They shall use real name and when relevant, role at TAJGVK.

12.1.2 Maintain Confidentiality

i)Professional use of social media sites:

- Employees/contractors shall be aware that social media usage is visible to clients, peers and senior management.
- Employees/contracture shall be truthful towards company.
- Employee shall not publish confidential information; confidential information includes things such as unpublished details about our software, details of current projects, and financial information.
- Employee shall respect the wishes of TAJGVK corporate customers regarding the confidentiality of document/projects.
- Employee shall always take approval from respective information owner to post or upload information documents related to TAJGVK.

ii)Personal use of social media sites:

- Employees/contractors shall use respectful language and be tolerant towards other views.
- They shall not post comments on sensitive topics such as religion, politics, sexual relations etc.
- Employees/contractors shall ensure that any content they publish must be true and not misleading, and all claims must be substantiated and approved.
- Employee shall not upload post or forward any content belonging to a third party unless they have third party's approval.

12.1.3 Use of disclaimers and adhere to copyright

- If employees/contractors are making any statements or decisions on behalf of TAJGVK, they shall make clear that statements are solely own.
- Employee/contractor shall always respect the laws of copyright and shall use copyrights material fairly which is owned by others.

12.1.4 Clarify statements that are misinterpreted

- Employees/contractors shall always keep in mind that what they write is their responsibility and failure to abide by these guidelines could put their employment at risk.
- Employee shall review the social media site after they have posted comments or contents. In case of misinterpretation, employee shall clarify them immediately.

12.1.5 Security measures to be taken care

- Employee shall always log out from the social media once they are not using.
- Employee shall ensure that credentials are not marked as 'Remember me'.
- History and cookies shall be deleted after successful log out from social media.

12.2 Company responsibility

- TAJGVK shall be clear on the social media policy, business objective and corporate culture. Social media policy shall be aligned with the goals and values of the organization.
- TAJGVK shall ensure that employees/contractors are aware of the company police to use social media websites.

12.2.1 Continuous monitoring and logging

- TAJGVK shall monitor the usage of social media and record the activities. TAJGVK shall monitor the posts related to TAJGVK and validate.
- TAJGVK shall conduct training and awareness program on do's and don'ts corresponding to use of social media.
- TAJGVK shall encourage employees to use disclaimer on their personal communications if related to organization information or asset.
- TAJGVK shall continuously monitor and update social media policy to ensure it meets legal requirements and reflects best practice.

- TAJGVK shall block all the social websites which is involved in pornography, entertainment and other unethical content.
- Bypassing any of TAJGVK's security mechanisms to access sites that are involved in pornography, entertainment or other unethical content is strict prohibited.

12.2.2 Take disciplinary action

- TAJGVK shall take necessary action in case any employee/contractor does not adhere to company policy.
- TAJGVK shall undertake a more detailed investigation in case evidence of misuse is found. In case of criminal activities, company shall report to police.

12.3 Applications and Benefits

12.3.1 External use of public social media

Firms are increasingly using public social media for a variety of business purposes, including:

- Building and maintaining professional relationships around with current and future clients
- Driving recruitment efforts
- Creating communities of alumni to help in obtaining new business referrals and re-recruitment
- Positioning the firm as a thought leader in areas such corporate responsibility
- Increasing awareness and knowledge on the firm's products and services and areas of expertise among potential clients and members of the public
- Showcasing of the firm's expertise and innovation hence generating referrals
- Personalizing the expertise of the firm by sharing the knowledge of high-profile leaders with the wider public

12.3.2 Internal uses of social media

Social media can also be used to improve the knowledge sharing, efficiency and quality of interactions within an organization. It is being seen as a new, more efficient way to handle business interactions that professionals do every day – attending meetings, participating in conferences, talking to clients. Social media can act as a platform for individuals of an organization to brainstorm, share ideas to ultimately raise the level of knowledge within a group.

12.4 RACI

Activities	Employee/Contractor	Marketing Team/ Media Team	Information Security Manager
Awareness to use social media	R / I	R / A	A / C
Social media	-	R	A / C

monitoring			
Security breach while use of social media	R	A / I	A

Notes:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

13 Supplier Relationship

13.1 Information security in supplier relationships

• TAJGVK should identify the information security control to specifically address the supplier's access to TAJGVK's asset and information.

13.1.1 Information security policy for supplier relationships

- TAJGVK shall implement standardize process and lifecycle for managing supplier relationship. Access to information and system shall be given as per the type of information system.
- An agreement shall be signed by supplier and TAJGVK upon the access to facilities and information and document the risk associated with the supplier's access to TAJGVK's information and system.
- TAJGVK shall review or develop a supplier life-cycle process, including initial reviews, monitoring, validation and ongoing assessments.
- TAJGVK shall conduct awareness training for both the TAJGVK's staff and supplier staff that handle or interact with data must be addressed.
- TAJGVK shall focus on establishing setup for conducting virtual training and awareness sessions for remote employees.

13.1.2 Addressing security within supplier agreement

- TAJGVK and supplier shall establish and document agreement to ensure that there is no misunderstanding between TAJGVK and supplier regarding both party's obligation to fulfil relevant information security requirements.
- Supplier activities i.e., access, process, store, communicate shall be included in the agreement.
- TAJGVK shall define acceptable uses for the data handled by the supplier.
- TAJGVK shall ensure that data classification requirements also apply to supplier
- TAJGVK shall define processes and procedures for monitoring compliance with the contract requirements.

13.1.3 Information and communication technology supply chain

- TAJGVK shall define the requirements of information security to address the information security risk associated with information and communication technology and product supply chain.
- TAJGVK should ensure that supplier activity and the product supply chain can be traced throughout.

13.2 Supplier service delivery management

13.2.1 Monitoring and review of supplier services

- Security controls and service levels, associated reports and records of third-party service providers shall be independently assessed, reviewed and monitored.
- Vendor audits shall be performed at least annually to review the services offered by the third party.
- Supplier shall promptly notify regarding security incidents.
- TAJGVK shall monitor service capability levels to ensure that the supplier continues to meet the contract terms and needs of the business.

13.2.2 Managing changes to supplier services

- Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
- TAJGVK shall consider the following items for managing changes in supplier system-
    - Service enhancements
    - Bug fixes
    - Use of new technology
    - New development tools
    - Enhanced security measures
    - Change of sub-contractor
    - Change of physical sites

13.3 RACI

Activities	Supplier	Information Security Manager	CMISF
Information security policy for supplier relationships		R	A
Addressing security within supplier agreements	I	R	R / A

Information and communication technology supply chain		R	A
Monitoring and review of supplier services		R	R / A / C
Managing changes to supplier services	C	R	R / A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

14 System Acquisition, Development and Maintenance

14.1 Security requirements of Information Systems

To ensure that information security is an integral part of information systems across the entire lifecycle which provide services over public networks.

14.1.1 Information security requirements analysis and specification

- Security requirements in an information system shall be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. They shall be justified and agreed with business process owners.
- Systems security requirements shall reflect the business value of the information assets involved (in accordance with the Asset Classification Policy and Procedures) and the potential business damage that may be caused due to absence of enough security. Where applicable, the policy and procedures may include and abide by the applicable laws.
- TAJGVK shall ensure the security of information asset with regards to confidentiality, integrity and availability.
- TAJGVK shall ensure that appropriate level of access shall be provided to employee/contractors for information and information processing facilities.

14.1.2 Securing application services on public networks

- Application services containing confidential information should be passed through a secured and authorized network which should be protected from contract dispute, unauthorized disclosure.
- Information passing over public network should be encrypted using cryptographic technique and only authorized person should have the decryption key. Also, the organization should ensure that there is no data loss in the information system while passing over public networks.
- TAJGVK shall provide a full suite of network security services including network security testing such as secure code review, vulnerability assessment and penetration testing, security consulting services.

- TAJGVK shall protect the confidential information from network attacks while passing over public networks. Passive attack- Wiretapping, port scanner, idle scans etc.
- TAJGVK must use secure protocol services and block cleartext protocol services such as FTP, Telnet, etc.
- Active attack- Denial-of-service attack, Spoofing, Man in the middle, Smurf attack, Buffer overflow etc.

14.1.3 Protecting application services transactions

- TAJGVK should protect information involved in application service transactions against incomplete transaction, misrouting, unauthorized message alteration, unauthorized disclosure or duplication.
- TAJGVK shall ensure that transaction details are stored in a secured place.
- TAJGVK may review and consider the following security functions for application service transactions
  - Entitlements Service for Authorization
  - Verification Service for Digital Signatures
  - Privacy Service for End-to-end Encryption

14.2 Security in development and support processes

The organization should ensure that information security should be designed and implemented within the development life cycle of information systems.

14.2.1 Secure development policy

- TAJGVK should set a procedure for the development of software or system in a secure environment within the organization. Secure development of software or system includes secure network, service and architecture.
- TAJGVK shall ensure that code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.

14.2.2 System changes control procedure

- Changes to systems with the organization should be well documented and enforced to ensure the integrity of the system, application or products.
- A formal process should be followed for documentation, specification, testing, quality control, and managed implementation.
- TAJGVK should monitor the changes to be aware of the impact of the changes to the system.

14.2.3 Technical review of applications after operating platform changes

- After changes or modifications in the operating platform, all the business functions should be reviewed to make sure that no adverse impact on organization security.
- TAJGVK shall review the application control and integrity procedures to ensure that they have not been compromised by the operating system changes.
- TAJGVK shall ensure that appropriate changes are made to the business continuity plans.

14.2.4 Restrictions on changes to software packages

- Application packages or software function should be defined by TAJGVK. Changes should be done with only administrative privileges and any unauthorized access should be restricted.
- If a change or update is required, it is recommended the impact should be analyzed and approved by the respective department head.
- TAJGVK shall prevent executable files from running on the local computer, organizational unit, site, or domain.

14.2.5 Secure system engineering principle

- Secure information system engineering procedures based on engineering principles should be well documented, established and applied to in-house information system.
- The implemented engineering principle should be continuously monitored to ensure that they are effectively contributing to enhance standards of security within the organization.
- TAJGVK shall protect information while being processed, in transit, and in storage.
- TAJGVK shall isolate public access from critical information or system.
- TAJGVK shall authenticate users and processes to ensure appropriate access control decisions both within and across domains.

14.2.6 Secure development environment

- TAJGVK should establish a secure development environment for system development and integration effort that cover entire product life cycle.
- A secure environment consists of authorized personnel, process and technology associated with the system development and integration.

14.2.7 Outsourced development

- Continuous monitoring and supervising of daily activity of outsourced system development.
- TAJGVK shall ensure that application code or development practice is accessible by authorized personnel only.

14.2.8 System security Testing

- A full testing and verification is required for new or updated system during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.
- For in house developed device, testing should be done by development team initially to ensure the expected output.

14.2.9 System acceptance Testing

- System acceptance testing should include testing of information security requirements and adherence to secure systems development practices.
- Acceptance testing should be performed in realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment.

14.3 Test data

TAJGVK should protect the test documents from unauthorized personal.

14.3.1 Protection of test data

- The data or documents used for testing contain confidential information and it should be protected from unauthorized employees or contractor.
- All sensitive details and content should be protected by removal or modification.
- TAJGVK shall refresh test data that helps to improve testing efficiencies and streamline the testing process while maintaining a consistent, manageable test environment.

14.4 RACI

Activities	Employee/ contractor	IT Team	CMISF / IT Head	Information/ Asset owner
Information Security requirements	I	I	R	R / A
analysis and specification				
Securing application services on public networks	I	R	R / C	A
Protecting application services transactions	I	R	R / C	A
Secure development policy	R	R	R / C	A / C
System changes control procedures	I	R	R / C	A
Technical review of applications after operating platform changes			R	A / C
Restrictions on changes to software packages	R	C / R	C	A
Secure system engineering principles	R	R	R / C	R / A
Secure development environment	R	R	R / C	A
Outsourced development			I	R / A
System security testing		R	R / C	A
System acceptance testing			R	R / A
Protection of test data	R	R	R / C	R / A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

15 End User Acceptance

15.1 Awareness about information security

- TAJGVK shall ensure that rules and policies related to information security are communicated to employees/contractors.
- End user shall follow the policies related to use of TAJGVK's asset.
- Employees/contractors shall ensure that TAJGVK's asset are being used only for business and operational purpose
- End user shall always keep information confidential and shall not share with unauthorized personnel.
- TAJGVK shall conduct training programs to communicate information security guidelines through on-premise and virtual setup for remote employees.

TAJGVK Should revisit security measures on remote working employees with a higher risk to cyber-attacks.

15.2 Acceptable use of information facilities/assets

• End user (employee/contractor/third party) shall aware of the policy regarding to acceptable use of information assets.

15.2.1 Use of laptop/desktop/mobile

- End user shall always take care of the following activities in order to use TAJGVK's asset-
    - Lock the desktop/laptop when not in use
    - Lock or log out from office phone when not in use
    - TAJGVK's asset shall always be kept in user's premises
    - Antivirus shall be updated in user's system and additional changes will not be done without approval from asset owner
    - Use shall not use external devices (USB, disk etc.) in order to prevent malware and virus attack
    - User shall always use the asset for which they have authorization.
    - User working remotely should update their device login password regularly.
    - Turn off the VPN on remote device when not required.
    - Remote user should make sure they are logged in via secured home network.

15.2.2 Use of applications/software

- User shall not download or install any unlicensed copy to TAJGVK's system
- Approval will be required in case of any required software installation/uninstallation.
- User shall not change the settings for installed applications.

15.2.3 User password policy

- User authorization shall be required in order to access organization's information.

- Password for the authentication should contain at least 8 characters including special characters and numbers.
- In case of first use, TAJGVK shall provide one time password, and shall be forced to change as per organization
- policy.
- End user shall always keep their passwords very confidential. Password shall not be guessable.
- User shall change password in regular intervals to prevent unauthorized access.
- Multiple device authentication should be required for remote employees for login to official laptops.

15.3 Use of internet/intranet

- • TAJGVK shall define process to acceptable use of internet or intranet. End user shall always follow the following activities while using internet/intranet connection:
    - Restrict all communication to and from the Internet with TAJGVK LAN and WAN network through the Firewall.
    - All internet communication is logged, monitored and audited periodically.
    - Ensure that users are granted access for business purpose only after formal approval procedure.
    - Users are informed about the purpose of corporate Internet connection, unacceptable use and cautions, copyright issues and disciplinary action for violation of acceptable use policy and general Internet ethics.
    - Ensure that all Internet connections to and from the internal computers shall be filtered at the firewall.

15.4 User physical security

- TAJGVK shall ensure that physical security policy is communicated to end users.
- End user shall always carry access card/identity card before entering into TAJGVK premises.
- Contractor/third party shall always enter his details in register provided at the entrance.
- Employees shall be prevented from tail-gating.
- Security personnel shall always check user's bag and validate the organization's asset details.
- User shall always keep information document in a secure place.
- While using TAJGVK's asset for printing or scanning, authorization shall be required and user should stay there until the work is done.
- User shall share the documents and keep a back-up before disposing them. Approval shall be required before disposal.
- User shall not eat, drink and smoke at workstation.

15.5 RACI

Activities	End User (Employee/contractor)	Information owner	Network / IT/Information security manager
Awareness about information security	I	R / A	R / A
Acceptable use of organisation asset/ information	R	R / A	R / A / C
Physical Security	R / I	R	C

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

16 Cryptography and Key Management

16.1 Cryptography Controls

• TAJGVK shall use cryptographic control effectively to maintain confidentiality and protection of information.

16.1.1 Policy on the use of cryptographic controls

- TAJGVK shall implement encryption algorithm to maintain confidentiality and protect information from unauthorized access.
- Based on type of risk, the required level of protection is identified, and encryption algorithm is implemented accordingly (e.g., CC Details, PII, Backup etc.)
- Cryptographic controls are used to achieve confidentiality, data integrity, non-repudiation, authentication etc.
- A proper key management system shall be implemented to decrypt the information to use.
- Cryptographic controls are important to minimize the risk and maximize the profit and to avoid inappropriate use.
- Encryption shall be used for transportation of information by mobile devices and removable media devices or across communication lines.
- Roles and responsibilities shall be defined for key management and implementation of policy
- Encryption shall be adopted for information assets based on the criticality of information. Standard encryption technology would be deployed for encryption unless required by regulatory requirements.

16.1.2 Key Management

- TAJGVK shall manage the use, protection and lifetime of cryptographic keys. TAJGVK shall ensure the whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying the cryptographic keys.
- Cryptographic keys shall be protected against loss and modification. Only authorized personnel should have access to the keys.
- The validity and relevance of the cryptographic keys should be ensured by revoking the ineffectual key and generating a new key (or key pair), when appropriate.
- The secret key shall be secured by logically and physically securing the device on which the key is stored.
- The shared secret key shall be accessible only by authorized personnel on a need-to-know basis.
- Keys shall be revoked and generated afresh in case of suspected compromise.
- Audit trails of key management activities shall be stored and protected.
- Internal Certification Authority systems shall be managed securely with appropriate physical and logical controls.
- Secure backup of private keys shall be maintained on an independent secure media which provides a source for key recovery.
- Backed up keys shall be protected from physical and environmental threats.
- Cryptographic keys shall be destroyed in a secure manner when they are no longer required.
- No copy of user's private key shall be retained by the internal Certification Authority to avoid risk of repudiation.
- Users shall keep their private keys strictly confidential and shall be responsible for the safety of their private keys.

16.3 RACI

Sr no.	**Activities**	Information Security Team	CMISF
1.1.1	Policy on the use of cryptographic controls	A	R
1.1.2	Key Management	R	A

Note:

R-	Responsible	A-	Accountable	C-	Consulted	I-	Informed

17 Cybersecurity Policy

17.1 Data Protection

Weak data protection increases the likelihood of leaking confidential business information to unauthorized parties.

Without a formal policy on how to manage mobile devices, users may not take appropriate security measures to protect mobile devices.

- Deploy Data Loss Prevention (DLP) tool to identify, analyses and mitigate data leakage incidents occurring in the TAJGVK environment.
- Define ownership of data for each business function based on the data classification standard
- Enterprise-wide data sanitization or anonymization techniques to be exercised to prevent unauthorized access to critical information which includes the following steps:
    - Identify and classify the critical data according to its confidentiality in order to recognize the sensitive data that cannot be shared outside of the organization.
    - Map the information systems/ applications that hold such sensitive information
    - Prepare the scope accordingly and implement controls to sanitize the same
- Implement an enterprise-wide documented cloud security policy/ checklist
- Strengthen MDM solution/ tool capabilities for secure handling of data on mobile devices. Consider the following:
    - Enable Remote wipe data
    - Review and update the MDM policies periodically
- In case of electronic portable media (USBs, flash drive, etc.) exceptional approval should be tracked and reviewed periodically.

17.2 Network Security

A lack of network segregation could allow security issues originating from less trusted devices or components to further spread to core infrastructure. Poor authentication mechanisms increase the risk that an unauthorized user can gain access to the network.

- No Information System shall be exposed to the Internet without a firewall.
- All Information Systems, which require being accessible from the Internet must be deployed in a DMZ (Demilitarized Zone).
- Segregate the network to minimize the risk of any security breach. Use of VLANs while performing network segregation is advisable.
- Network segregation according to the business functions should be performed to directly decrease the number of systems on the same network segment, thus reducing device network processing and malicious reconnaissance.
- Where possible, network monitoring tools must be used to trigger alarms, alerting the Company when suspicious activity occurs.
- Where possible, systems must be synchronized with a time server.
- Deploy Network Access Control (NAC) solution with CA certificate. Implement MAC binding on-site in addition to NAC solution.

- All system, administrative and user activities must be logged on Information Systems as mandated by TAJGVK.

17.3 Third Party Management

Lack of a centralized repository increases the risk that vendor contracts are not being managed effectively. As a result, ownership and accountability of third-party vendors are not consistently established. Without having a central procurement function to handle third-party contracts, teams could vary their process for engaging third parties, and all necessary steps to manage risk may not be followed.

- Conduct vendor risk assessments for critical vendors. Also, it is recommended that during the vendor relationship, all vendors should be reviewed on an ongoing basis based on the risk category.
- Information security clauses should be included in vendor contracts.
- Third party vendor management framework should be defined and implemented by all business units which cover the following topics:
    - Procurement workflow mechanism to be defined
    - Vendor risk rating model to be designed and implemented as part of the procurement process as well as in the contracts.
    - Sub-contracting and escalation mechanisms to be defined
- Outsourced activities must be subject to adequate supervision and management review.
- The contract must have all the necessary security conditions and service levels to ensure compliance with the security policies. The following terms must be considered for inclusion in the contract:
    - Controls to ensure safekeeping, return or destruction of information assets at the end of, or at an agreed point in time during the contract.
    - Restrictions on copying and disclosing information.
    - Approval from TAJGVK Management for further subcontracting above appropriate thresholds.
    - The respective liabilities of the parties to the agreement.
    - Intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work like development of software/application.
    - The right to audit.
    - Compliance with the TAJGVK policies.
    - Compliance with software licensing agreements and use of licensed tools/methodologies to carry out the agreement.
    - Indemnification of TAJGVK in case of breach of any third-party licensing agreement or third party IPR by the vendor.

17.4 BCP/ DR

In the absence of a BCP framework, critical processes and users defined in the organization may not be able respond to the disaster in a structured and timely manner

- Define, document and test Business Continuity (BC) framework and plan documents vis-a-vis ISO 22301 standard. Framework documents shall include, but not limited to, the below:
    - Business continuity policy manual,
    - DR drill calendar should be maintained, and Drills need to be carried out on a regular basis
    - Need to implement Crisis management plan
    - Governance structure and procedure
    - Risk management procedure (to be integrated with the risk management policy)
    - Business impact analysis procedure
    - It is recommended that the staff experience, resource count and budget are to be considered for BCM initiatives.
    - All backup media identified critical infrastructure and applications must be stored in a secured manner in a fireproof storage area.

17.5 Awareness

Internal users can create information security vulnerabilities through lack of awareness of attacker tools and exploits, and unintentional misuse of information systems. If user awareness and education on information security policies and procedures are not performed, then it poses a great harm to the security of the company.

- It is recommended that Information security awareness trainings to be made mandatory for the internal employees, contractors and temporary staff. Also, any company personnel that were hired prior to the roll out of the security training awareness program should take on - boarding security training.
- Define a formal security training awareness program across locations. Effectiveness of the trainings should be measured and reported periodically. Additionally, review and update the security awareness training program on a periodic basis.
- Develop calendar to plan and conduct security trainings and awareness. Ensure refresher trainings are provided on pre-defined timeline.

17.6 Governance and Organization

Without an information security governance organization, security risks may be inconsistently treated and monitored, resulting in increased vulnerabilities with less visibility into the environment. There is a risk that business functions and IT teams may fail to collaborate with each other to identify and respond to threats and vulnerabilities

- Information security roles and responsibilities should be formally defined and documented. TAJGVK should consider having full/ half information security FTEs to form as dedicated team.
- Form a governance structure covering representative from all business functions, inclusive of executive management to help bridge the gap between business and security.

- Applicability of information security compliances (GDPR, PCI-DSS) to be mapped in the tool (Legatrix).
- Establish a risk assessment methodology to assess risks and critical processes. This methodology should include the following:
    - Risk definitions and exposure/ impact information
    - Definition of the risk landscape/ universe (including third parties, technology and facilities)
    - Risk acceptance criteria
    - Risk treatment/ remediation plan
    - Establish ownership of the key risk areas

17.7 Asset Management

The organization cannot provide solutions to protect its confidential and critical systems if it does know what those systems are and where they reside. Also, IT security processes such as vulnerability management, compliance management and disaster recovery planning depend upon an accurate asset inventory to verify critical information and infrastructure are covered by those processes.

- It is recommended to maintain a centralized consolidated asset inventory capturing all IT components/ information assets and identify critical vs non-critical assets. Include software assets, applications and paper assets in the inventory along with software licenses and review the inventory regularly.
- Document and roll-out supporting policies and procedures for classifying assets based on criticality of the data processed by such systems across the organization.

17.8 Architecture

Without a robust architecture function, organization might not be aware of how new changes or modifications might affect the functionality of the entire organization and understand critical infrastructure points that need to be protected

- All network designs must be documented, approved from security and maintained.
- The documentation must include a current network diagram that illustrates all connections to components that process or store confidential information, e.g., credit cardholder data, including any wireless networks must be developed and maintained.
- Security architecture function should be formally defined through policies, procedures and standards which can meet business goals.
- Changes to systems, network designs, technology components, etc. should be always reviewed for security risks by the security architecture function.

17.9 Host Security

If assets without end-point protections are not identified, tracked and resolved, there is no security solution in place to catch known exploits. Hence, there is an increased risk that malicious users or attackers may be able to exploit vulnerabilities on the assets and use the assets as an entryway into the organization's internal network.

- It is recommended to enhance Anti-Virus by behavior-based technology. Also, alerts to be configured for incidents and policy scans to be automated and scheduled periodically on the existing AV console.
- Patching to all end points should be done along with maintaining a list of applied and rejected patches. Applied and rejected patches should be tracked and reported regularly
- Mechanism to track and report configuration baselines needs to be defined and followed in the organization in order to ensure implementation of security baselines in a structured manner.
- It is recommended to track and monitor the USB exceptions to ensure compliance with information security policy.

17.10 Identity and Access Management

Without an enterprise wide IAM strategy, there may be no visibility into the program or consistency in IAM processes, tools and technologies. If privileged account authenticators are not adequately protected, there is an increased risk that privileged accounts may be more easily compromised.

- Identity and access management is formally defined.
- Single Sign-On (SSO) platform has been integrated with the IAM process. Furthermore, we noted that for privilege accesses, ARCON-PIM is used.
- For the O365 application and privileged access, multi-factor authentication has been implemented and it is OTP based which is managed by the HO office.
- Broaden multi-factor authentication use to remote access to corporate access.
- Review of User access rights should be carried out on a periodic (Recommended to be performed quarterly or bi-annually) basis.

17.11 Operations

Failure to implement and maintain sufficient physical security can lead to physical compromise resulting in data confidentiality, integrity and availability being compromised.

Insufficient testing, approval and segregation of duties could result in unauthorized changes, or changes that adversely impact the production environment, being implemented

- Regularly log and monitor physical access activity at the organization especially critical infrastructure such as Data center. The access activity is required to be periodically reviewed.
- Ensure that physical security controls such as visitor management, asset declaration are consistently followed vis-s vis the TAJGVK policy.
- Physical security controls for visitors should be followed consistently.
- Change management process should be formally defined and documented. Post implementation test for all infrastructure and application related changes must be performed. Information security related test should be a part of the same process to ensure security requirements are met.

17.12 Privacy

The lack of specific policies, standards or procedures governing the uses of personal information may result in the improper use or disclosure of information in violation of corporate privacy policies and localized privacy laws and regulations

- Develop/update a data disclosure policy capturing privacy requirements and the same should be communicated to respective stakeholders.
- The privacy breach management process to be defined and monitored for effectiveness.
- Additionally, specialized training for privacy related incident response is to be provided to the personnel handling incidents related to PII or SPI data
- Perform privacy assessment to analyses country wise privacy requirements and compliance to local laws.
- Data Privacy officer should be registered with appropriate authority for the region.

17.13 Security Monitoring

Lacking an overall strategy for security monitoring will likely result in disparate and siloes attempts to fight an increasing number of vulnerabilities. Without regular security monitoring reporting, TAJGVK may not have the information and intelligence required to make informed decisions on, and changes to security monitoring strategy, people, tools or processes.

- It is recommended that applications are integrated with SIEM to facilitate continuous monitoring for application logs.
- Log management policy should be defined as per the following topics:
    - Log lifecycle (controls like log format, encryption, etc.)
    - Data retention period mapping to business requirements which includes
    - Short Retention Period: This applies when a business need is not present to retain data for the full length of the Standard Retention Period and has confirmed that a Prolonged Retention Period does not apply. In that case, it is the responsibility of the relevant member of staff to delete the data.
    - Standard Retention Period: This applies by default if no action is taken by the relevant member of staff and entails the deletion of emails within a <defined time period> of their creation and documents within a <defined time period> of their creation.
    - Prolonged Retention Period: This applies when a legitimate business needs to retain the data for longer than the Standard Retention Period or a legal requirement to retain the data applies.
    - Archival of data (For ex: data retention schedule)
    - Log policy reviews and audit considerations

17.14 Threat Intelligence

Lack of a cyber threat intelligence program increases the risk that threats may not be proactively identified before they cause material harm. Also, absence of documentation for CTI function will result in ineffective threat management.

- Conduct regular threat intelligence assessments in order to ensure no critical data is freely available on the internet universe

- It is recommended that the targeted determined adversaries/ attackers (e.g., the APT) program and vendors should be evaluated by the organization
- It is recommended that the support from the leadership with a defined budget should be present to strengthen the cyber threat intelligence capabilities.
- Understand cyber threat intelligence and define an organization wide threat intelligence framework, roles and responsibilities

17.15 Vulnerability Identification and Remediation

Lacking an overall strategy for threat and vulnerability management will likely result in disparate attempts to fight an increasing number of identified vulnerabilities and unknown threats.

- A comprehensive set of procedures and guidelines for vulnerability management need to be defined and documented based on the following topics:
    - Current workflow mechanism to be defined
    - Steps to remediate the vulnerabilities identified and post remediation review process to be defined
    - Mapping of IT operation processes that are integrated with the vulnerability management process to be conducted
    - Define and implement metrics for vulnerability identification and remediation.
- It is recommended that the assignment ownership for rectifying the vulnerabilities should be done regularly.
- Define and implement a standard policy to perform attack and penetration assessments on any new or emerging technology before it is embraced along with a risk-based schedule to test the existing applications and infrastructure.

17.16 Metrics and Reporting

Without sufficient visibility into information security metrics, the Board may not provide adequate support for information security objectives, policies, programs or initiatives. Executive support is a key driving factor in making information security an integral part of the company's business and operations.

- Define standardized and actionable KPIs for periodic security measurement and reporting. Establish a formal metrics program review.
- Regularly review IT security controls efficiency.
- Define the process for managing non-conformance to defined benchmarks and targets.

17.17 Policy and Standards

Absence of security policies will cause lack of consistency in day-to-day operations. In addition, users may not comply with required processes and controls, which may increase the risk of a breach.

- Establish a formal process for managing the policy exceptions to information security. Additionally, global security exceptions should include corporate visibility and approval. Process should be established for reviewing and updating the Information Security Policies.

- Increase the involvement and ownership of the business and IT in the PSGs. It is recommended that the implementation of Policies, Standards and Guidelines should be made consistent across all regions.
- Perform information security review against the existing policies and procedure to measure the effectiveness of the defined process
- Define a process to evaluate and formulate key performance indicators (KPIs) for the information security program

17.18 Strategy

Information security risks may go unidentified or unaddressed in the technology environment or regarding the people component, and therefore, risks may be inconsistently treated, managed, monitored or mitigated. This could lead to unintentional exposure to vulnerabilities that may have an enterprise impact. The information security budget may be misallocated.

- Information security strategy should be pre-planned and created in detail to provide support in any major initiative. Also, the communication should be in simple business language for effectiveness.
- Plan and hold an IS steering committee which includes members from all business functions on a formally defined periodic basis to discuss information security initiatives and metrics.
- Define and implement a proper linkage between information security strategy, IT and business objectives

17.19 Incident Response

Without a formally established incident response team, the organization may not have the adequate and dedicated resources required to respond to incidents in a timely manner.

- Define and implement security incident classification and categorization standard for identification and detection of major incidents.
- Incident response plans for specific IT security scenarios (such as malware attack, DDoS attack, phishing, etc.) should be documented to enable the response teams to take appropriate actions.
- A program for regular exercises or tests to determine existing capabilities to respond to a major security incident should be established.

18 Privacy by Design

18.1 Purpose

This policy is for employees, workers, and contractors of TAJGVK Hotels and Resorts Limited (hereafter referred to as “TAJGVK” or “us” or “we”). When processing personal data (defined below), TAJGVK obliges to implement appropriate technical and organizational measures (taking into consideration the nature of the processing, risks to individuals and costs etc.), into such processing activities in order to meet the requirements of the data privacy laws and protect the rights of the data subjects concerned. The ‘appropriate measures may change from one processing activity to the other, and it is important that such measures are given consideration at the start of,

and throughout, the life-cycle of TAJGVK's processing of personal data. This obligation is referred to as 'Privacy by Design'. As a minimum, such measures must ensure that only personal data which are necessary for each specific purpose of the processing are processed and that the personal data is not made available to an indefinite number of individuals without the data subject's consent.

This Policy provides guidance on TAJGVK's approach to ensuring that it embeds privacy by design across TAJGVK's operations. Since 'Privacy by Deign' is a vital requirement of the data privacy laws, it is important that all staff understand and implement this Policy.

If you have any questions, please contact TAJGVK's Infosec team at <TAJGVK@TAJGVK.com>.

18.2 Definition

Term	Definition
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject')
Special Category of Personal Data	Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. For the purpose of this policy, when we are referring to 'personal data', we are referring to Personal Data and Special Categories of Personal Data collectively.
Data Protection Impact Assessment (DPIA)	An assessment of the impact of the processing operations on the protection of personal data as referred to under Art 35 of GDPR;

Processing Principles	Means the processing principles set out in Art 5 of GDPR and as attached as an Appendix to this Policy.

18.3 Privacy by Design – General Principles

The principles of 'Privacy by Design' can be summarized as:

#	Principle
1	Use proactive rather than reactive measures. Anticipate, identify, and prevent privacy invasive events before they happen.
2	Privacy should be the default position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy.
3	Privacy must be embedded and integrated into the design of systems and business practices.
4	All legitimate interests and objectives are accommodated in a positive-sum manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5	Security should be end-to-end throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.
6	Visibility and transparency are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
7	Respect user privacy by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user-friendly options.

18.4 Technical and Organizational Measures

- TAJGVK's aim is to implement appropriate technical and organizational measures which are designed:
    - to implement the Data Protection Principles in an effective manner, and
    - to integrate into the processing of personal data the safeguards necessary for that purpose.
- This Policy applies at the time of determining the means of processing, and at the time of actually processing the personal data.
- In doing so, TAJGVK will consider the available technical and organizational measures, the cost of implementation and the nature, scope, context and purposes of processing of personal data, as well as the risks of varying likelihood and

severity for rights and freedoms of individuals presented by the processing of their personal data.

- If it is considered that the processing presents a high risk to individuals, a DPIA must be carried out in accordance with TAJGVK's data privacy policy.

18.5 Privacy by Default

- TAJGVK's aim is that appropriate technical and organizational measures will be applied to ensure that, by default, only the personal data which is necessary for each specific purpose of processing of personal data is used, in relation to:

  (a) the amount of personal data collected;
  (b) the extent of processing that personal data;
  (c) the period of its storage; and
  (d) its accessibility.

- TAJGVK's aim is that by default personal data should be restricted to those who have a business need to know.

18.6 Data Protection by Design

- TAJGVK's aim is that when considering a proposal for a particular type of processing of personal data, the impact of this on the individuals affected should be considered, and that appropriate technical and organizational measures should be put into place to ensure that:

  (a) the Data Protection Principles are implemented; and
  (b) any risks to individuals' rights and freedoms are minimized.

- Vigilance by staff should be exercised continually to ensure the security of TAJGVK systems and personal data, e.g., against attempts to trick individuals into revealing their log-in details; and to avoid risks of personal data breaches arising from mobile devices and remote log-ins. Staff should avoid downloading, working with, or storing identifiable personal data wherever possible, and only undertake these activities in compliance with appropriate guidance and policies. Anonymized or partly/reversibly anonymized data should be used wherever possible.

- When buying systems/software which involve personal data or considering transfers/sharing of personal data including using the "cloud", staff must evaluate the privacy and security of alternative solutions and vendors/partners. The use of such systems/software should to the maximum extent possible avoid personal data being involved or put at risk of a data breach. Personal data should only be placed on systems, devices or software where this is compliant with TAJGVK's policies and the applicable legislation. The use, and duration of holding, of personal data should be minimized. Reviews of, and improvements to, privacy should be undertaken regularly by staff in their areas of work, documented, and privacy risks and precautions reviewed by staff regularly.

- Managers or staff should not purchase new systems or software without first reviewing their proposed use in terms of a Data Protection Impact Assessment if the proposed use presents a high risk to individuals, and the proposed purchase also requires to be checked first by Procurement and by Information Services for contract terms, and for the uses of, and risks to, personal data. For purchasing supplies/services, regardless of contract value, no managers or staff should

approve a contract with a supplier unless the terms have been checked for data protection compliance.

18.7 Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Ensuring overall compliance with the present policy • Ensuring each new initiatives follows the requirements defined in this policy • Providing support for risk assessment, recommendations, and Implementation of appropriate controls • Involved in the contract defining and reviewing process
TAJGVK IT team	• Developing the DPIA based on the availability requirements • Implementation of necessary security measure to comply with the security requirements defined in the present policy

18.8 Compliance and Enforcement

Periodic audits of compliance shall be conducted at least annually. Results shall be documented, and any deficiencies corrected.

18.9 Exception

Any exception to this policy must be documented and forwarded to the Chief Information Security Officer CISO for review and approbation, which needs to be vetted by CIO also.

18.10 Monitoring and Reporting

This document shall be reviewed once a year or at the time of any major change in existing environment affecting policy, whichever is earlier.

This document contains controlled copies of the procedure listed above. Any copies made from this document, in part or in whole, are uncontrolled and are therefore not subject to further review, revision or approval.

18.11 Appendix

Article 5: Principles relating to processing of personal data:

1.Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further

processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').