

Policy/Procedure	Description
<b>ISO 27002 Policies</b>	
Assessing Security Risks	The purpose is to ensure a risk assessment is conducted periodically and as needed.
Treating Security Risks	The purpose is to ensure that a determination is made on each risk identified in the risk assessment.
Information Security Policy Document	The purpose is to provide Management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Review of the Information Security Policy	The purpose is to ensure review of the Information Security Policy at regular planned intervals or whenever significant changes occur to the environment.
Management Commitment to Information Security	The purpose is to manage information security within the organization and ensure the support and commitment of management.
Information Security Co-ordination	The purpose is to ensure co-ordination of information security activities throughout the organization.
Allocation of Information Security Responsibilities	The purpose is to appropriately allocate responsibility for information security.
Authorization Process for Information Processing Facilities	The purpose is to define management authorization for new information processing facilities.
Confidentiality Agreements	The purpose is to ensure identification of all requirements for confidentiality, creates confidentiality agreements, and issues them to members of the workforce.
Contact with Authorities	The purpose is to ensure contact is maintained appropriately with relevant authorities.
Contact with Special Interest Groups	The purpose is to ensure contact is maintained with special interest groups focused on information security.
Independent Review of Information Security	The purpose is to ensure the review of information security controls and implementation.
Identification of Risks Related to External Parties	The purpose is to maintain the security of information and information processing facilities that are

	accessed, processed, communicated to, or managed by external parties.
Addressing Security when Dealing with Customers	The purpose is to ensure that all identified security requirements are addressed prior to providing customers access to information or assets.
Addressing Security in Third Party Agreements	The purpose is to ensure that agreements with third parties address all relevant security requirements.
Inventory of Assets	The purpose is to achieve and maintain appropriate protection of organizational assets.
Ownership of Assets	The purpose is to ensure that all information and assets are owned by a designated part of the organization.
Acceptable Use of Assets	The purpose is to ensure that rules are developed for the acceptable use of assets.
Classification Guidelines	The purpose is to ensure that information is classified appropriately.
Information Labeling and Handling	The purpose is to ensure that classified information is properly labeled.
Roles and Responsibilities	The purpose is to ensure that members of the workforce understand their security roles and responsibilities.
Screening	The purpose is to ensure that appropriate background checks are carried out for members of the workforce.
Terms and Conditions of Employment	The purpose is to ensure that all members of the workforce agree to terms and conditions of employment including information security requirements.
Management Responsibilities	The purpose is to ensure that members of the workforce are aware of security threats and concerns, their responsibilities and liabilities, and are equipped to support the organizational security policy.
Information Security Awareness, Education and Training	The purpose is to ensure that relevant members of the workforce receive appropriate information security education and training.
Disciplinary Process	The purpose is to establish the disciplinary process for employees that have violated security policies or have committed a security breach.

Termination Responsibilities	The purpose is to manage the termination of all members of the workforce in an orderly manner regarding information and information processing facilities.
Return of Assets	The purpose is to ensure the return of assets from all members of the workforce upon termination of employment, contract, or agreement.
Removal of Access Rights	The purpose is to ensure the removal of access rights to all information upon termination of employment, contract, or agreement.
Physical Security Perimeter	The purpose is to protect information and facilities through the use of physical security perimeters.
Physical Entry Controls	The purpose is to ensure that appropriate entry controls are utilized in secure areas.
Securing Offices, Rooms and Facilities	The purpose is to ensure design and application of physical security for offices, rooms and facilities.
Protecting Against External and Environmental Threats	The purpose is to ensure protection of facilities from external and environmental threats.
Working in Secure Areas	The purpose is to ensure the design and application of physical protection and guidelines for working in secure areas.
Public Access, Delivery and Loading Areas	The purpose is to ensure secure procedures regarding public access, delivery and loading areas.
Equipment Siting and Protection	The purpose is to prevent loss, damage, theft, or compromise of assets and interruption to activities.
Supporting Utilities	The purpose is to ensure the protection of the organization from power failures and other disruptions caused by failures in supporting utilities.
Cabling Security	The purpose is to ensure the protection of power and telecommunications cabling from interception or damage.
Equipment Maintenance	The purpose is to ensure that equipment is maintained so as to ensure its continued availability and integrity.
Security of Equipment Off-Premises	The purpose is to ensure accounts for the heightened and specialized risks of working on equipment off-site.
Secure Disposal or Re-use of Equipment	The purpose is to ensure that all items containing any

	form of storage media have had sensitive data and licensed software removed, securely overwritten, or permanently destroyed.
Removal of Property	The purpose is to ensure prior authentication for equipment, information, and software taken off-site.
Documented Operating Procedures	The purpose is to ensure that operating procedures are documented, maintained, and made available to all users who need them.
Change Management	The purpose is to ensure that changes to information processing facilities and systems are controlled and documented.
Segregation of Duties	The purpose is to reduce opportunities for unauthorized or unintentional modification or misuse of assets.
Separation of Development, Test, and Operational Facilities	The purpose is to ensure the separation of development, test, integration, staging, and production environments to reduce the risk of unauthorized access or changes to production systems.
Service Delivery	The purpose is to ensure that security controls, service definitions, and delivery levels included in third party service delivery agreements are implemented, operated, and maintained by the respective third party.
Monitoring and Review of Third Party Services	The purpose is to ensure that the services, reports, and records provided by all third parties are regularly monitored and reviewed, and that audits are carried out regularly.
Managing Changes to Third Party Services	The purpose is to manage changes to the provision of services taking criticality of business systems and processes into account.
Capacity Management	The purpose is to ensure the monitoring of capacity requirements in support of required system performance.
System Acceptance	The purpose is to establish acceptance criteria for new information systems, upgrades and versions, and to ensure suitable tests of systems are carried out prior to acceptance.
Controls against Malicious Code	The purpose is to ensure the implementation of detection, prevention, recovery controls, and user awareness to protect against malicious code.

Controls against Mobile Code	The purpose is to ensure proper controls are implemented regarding the configuration, authorization and use of mobile code.
Information Back-up	The purpose is to ensure the regular performance and testing of system and information back-ups.
Network Controls	The purpose is to ensure that networks are adequately managed and controlled to protect from security threats to networks and systems and the data they transmit and store.
Security of Network Services	The purpose is to ensure the identification of security features, service levels, and management requirements for all network services, both internally and externally provided.
Management of Removable Media	The purpose is to prevent unauthorized disclosure, modification, removal, or destruction of assets.
Disposal of Media	The purpose is to ensure the secure and safe disposal of media when it is no longer required and the adherence to documented procedures.
Information Handling Procedures	The purpose is to ensure the establishment of procedures for the handling and storage of information that protects the information from unauthorized disclosure or misuse.
Security of System Documentation	The purpose is to ensure the security of system documentation and to prevent unauthorized access.
Information Exchange Policies and Procedures	The purpose is to maintain the security of information and software exchanged within or with any external party.
Exchange Agreements	The purpose is to ensure the establishment of agreements for the exchange of information and software between the organization and external parties.
Physical Media in Transit	The purpose is to ensure the protection of media containing information against unauthorized access, misuse, or corruption during transportation beyond facilities.
Electronic Messaging	The purpose is to ensure that information included in electronic messages is appropriately protected.
Business Information Systems	The purpose is to ensure the development and implementation of policies and procedures to protect

	information involved with the interconnection of business systems.
Electronic Commerce	The purpose is to ensure protection form information passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
On-Line Transactions	The purpose is to ensure the protection for information included in on-line transactions.
Publicly Available Information	The purpose is to ensure the integrity of information made available on publicly available systems.
Audit Logging	The purpose is to ensure the recording of user activities, exceptions, and information security events to assist in future investigations and access control monitoring.
Monitoring System Use	The purpose is to ensure the establishment of procedures to monitor the use of information processing facilities.
Protection of Log Information	The purpose is to ensure the protection of logging facilities and log information against tampering and unauthorized access.
Administrator and Operator Logs	The purpose is to ensure the logging of system administrator and system operator activities.
Fault Logging	The purpose is to ensure that faults are logged and analyzed and that appropriate actions are taken.
Clock Synchronization	The purpose is to ensure that the clocks of all relevant information processing systems are synchronized to an official or industry best practice source.
Access Control Policy	The purpose is to ensure that an access control policy is established, documented, and reviewed based upon business and security requirements for access.
User Registration	The purpose is to ensure the organization follows a formal user registration and de-registration procedure for granting and revoking access to all information systems and services.
Privilege Management	The purpose is to ensure that the allocation and use of privileges will be restricted and controlled.
User Password Management	The purpose is to ensure that the allocation of passwords are controlled through a formal

	management process.
Review of User Access Rights	The purpose is to ensure the review of user's access rights at regular intervals.
Password Use	The purpose is to ensure good security practices by users in the selection and use of passwords.
Unattended User Equipment	The purpose is to ensure that unattended equipment has appropriate protection.
Clear Desk and Clear Screen Policy	The purpose is to ensure protection for papers, removable media, and screen viewing from inappropriate or unauthorized access.
Policy on Use of Network Services	The purpose is to ensure that users are only provided with access to the services that they have been specifically authorized to use.
User Authentication for External Connections	The purpose is to ensure appropriate authentication methods are utilized to control access by remote users.
Equipment Identification in Networks	The purpose is to ensure the use of equipment identification as a means to authenticate connections from specific locations and equipment.
Remote Diagnostic and Configuration Port Protection	The purpose is to ensure that access to physical and logical diagnostic and configuration ports is strictly controlled.
Segregation in Networks	The purpose is to ensure the segregation of groups of information services, users, and information systems on networks.
Network Connection Control	The purpose is to ensure the restriction of the ability for users to connect to networks that extend across boundaries.
Network Routing Control	The purpose is to ensure the implementation of network routing controls to restrict computer connections and information flows to those approved by the Access Control Policy.
Secure Log-on Procedures	The purpose is to ensure that access to operating systems is controlled by a secure log-on procedure.
User Identification and Authentication	The purpose is to ensure that all users have and use a unique User ID and that authentication techniques are suitable to substantiate the claimed identity of a user.

Password Management System	The purpose is to ensure that they systems for managing passwords are interactive and ensure quality passwords.
Use of System Utilities	The purpose is to ensure the restriction on use and tight control over the use of system utilities.
Session Time-out	The purpose is to ensure that inactive sessions will be shut down after a defined period of inactivity.
Limitation of Connection Time	The purpose is to ensure the implementation of restrictions on connection times to provide additional security for high risk applications.
Information Access Restriction	The purpose is to ensure access to information and application system functions by users and support personnel are restricted in accordance with the Access Control Policy.
Sensitive System Isolation	The purpose is to ensure that sensitive systems have a dedicated and/or isolated computing environment.
Teleworking	The purpose is to ensure that a policy, operational plans, and procedures are developed and implemented for teleworking activities.
Security Requirements Analysis and Specification	The purpose is to ensure the specification of business requirements for new information systems and enhancements to existing information systems include requirements for security controls.
Input Data Validation	The purpose is to ensure the data input to applications is validated to ensure that his data is correct and appropriate.
Control of Internal Processing	The purpose is to ensure that validation checks are incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
Message Integrity	The purpose is to ensure that requirements for ensuring authenticity and protection of message integrity in applications are identified and that appropriate controls are implemented.
Output Data Validation	The purpose is to ensure that data output from applications is validated and that the processing of stored information is correct and appropriate to the circumstances.
Policy on the Use of Cryptographic Controls	The purpose is to ensure the development and

	implementation of a policy on the use of cryptographic controls for protection of information.
Key Management	The purpose is to ensure the implementation of a key management program to support the use of cryptographic techniques.
Control of Operational Software	The purpose is to ensure the control of installation of software on operational and production systems.
Protection of System Test Data	The purpose is to ensure that test data is selected carefully, protected, and controlled.
Access Control to Program Source Code	The purpose is to ensure that access to program source code is restricted.
Change Control Procedures	The purpose is to ensure that the implementation of changes is controlled by the use of formal change control procedures.
Technical Review of Applications after Operating System Changes	The purpose is to ensure that whenever Operating Systems (O/S's) are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on the operations or security.
Restrictions on Changes to Software Packages	The purpose is to ensure tight controls regarding changes to software packages.
Information Leakage	The purpose is to ensure that opportunities for information leakage are prevented.
Outsourced Software Development	The purpose is to ensure the supervision and monitoring of outsourced software development.
Control of Technical Vulnerabilities	The purpose is to reduce risks resulting from exploitation of published technical vulnerabilities.
Reporting Information Security Events	The purpose is to ensure that information security events are reported through appropriate management channels as quickly as possible.
Reporting Security Weaknesses	The purpose is to ensure that all members of the workforce are required to note and report any observed or suspected security weaknesses in systems or services.
Responsibilities and Procedures	The purpose is to ensure the establishment of management responsibilities and procedures to information security incidents.
Learning from Information Security Incidents	The purpose is to ensure that the information gained

	from information security incidents is utilized to identify recurring and/or high impact incidents.
Collection of Evidence	The purpose is to ensure the collection and retention of evidence in cases where an information security incident requires legal action.
Including Information Security in the Business Continuity Management Process	The purpose is to ensure that information security requirements are addressed as a part of the business continuity process.
Business Continuity and Risk Assessment	The purpose is to ensure identification of events that can cause interruptions to business processes.
Developing and Implementing Continuity Plans Including Information Security	The purpose is to ensure the development and implementation of a business continuity plan.
Business Continuity Planning Framework	The purpose is to ensure that single framework for business continuity plan is maintained.
Testing, Maintaining and Re-assessing Business Continuity Plans	The purpose is to ensure that business continuity plans are tested and updated regularly and remain effective.
Identification of Applicable Legislation	The purpose is to avoid breaches of any law, statutory, regulatory, or contractual obligations, and any security requirements.
Intellectual Property Rights (IPR)	The purpose is to ensure compliance with all intellectual property rights requirements.
Protection of Organizational Records	The purpose is to ensure that important records are protected.
Data Protection and Privacy of Personal Information	The purpose is to ensure the protection of data and privacy in support of legislation, regulations, and contractual obligations.
Prevention of Misuse of Information Processing Facilities	The purpose is to ensure that users are deterred from using information processing facilities for unauthorized purposes.
Regulation of Cryptographic Controls	The purpose is to ensure that cryptographic controls are used in accordance with all relevant agreements, laws, and regulations.
Compliance with Security Policies and Standards	The purpose is to ensure compliance of all systems with security policies and standards.
Technical Compliance Checking	The purpose is to ensure that information systems are regularly checked for compliance with security

	implementation standards.
Information Systems Audit Controls	The purpose is to ensure that audit requirements and activities do not disrupt business processes.
Protection of Information Systems Audit Tools	The purpose is to ensure that access to information systems audit tools is strictly controlled.

Figure 1: Summary of ISO 27002 Policies