
SCHEDULE 3 – SECURITY REQUIREMENTS

01. Definitions

In this Schedule, unless the context otherwise requires the following expressions shall have the meanings set out below

Adapters	logical segregators which vary in shape and form, ranging from in-house developed software, off-the shelf software or specialised devices / environments (including firewalls, VLANs) as well as specific commercial arrangements etc.
Best Industry Practice	established methods, processes or approaches widely acknowledged and adopted for secure Information Systems.
Breach of Security	includes the occurrence of unauthorised access to or use of the Customer Premises and/or the Location, the Services, the Solution or any ICT or data (including the Customer's Data) used by the Customer or the Contractor in connection with the Agreement.
Business Continuity and Disaster Recovery (break-glass) account	Emergency access account that is highly privileged and is limited to emergency scenarios where normal administrative accounts cannot be used.
Contractor	entity hired by Customer to perform specific task or services under a contractual agreement.
Contractor Personnel	means the contractor's employees and subcontractors performing the services.
Contractor System	means the information and communications technology system used by the Contractor in performing the Services including the Software, the Contractor Equipment.
Customer	refers to the entity that has procured a Service or Solution.
Customer Data	refers to information and data which was provided or generated by the Customer during the course of using a Service or Solution.
Disaster	means the occurrence or the likely occurrence of one or more events which, either separately or cumulatively, mean that the Solution and/or the Services, or a material part of the Services, are or will be unavailable resulting in material disruption to business continuity of the Customer, including without limitation a disaster or Force Majeure.
Information System	An interconnected set of components used for collecting, storing, processing data and providing information.
Interactive highly privileged (super user) account	A user account that has the highest possible privileges in a Solution. Examples of super user accounts include the ' <i>root</i> ' account in Linux and Unix, and the ' <i>administrator</i> ' account in Windows.
Non Interactive Account	An account that does not require human interaction to access a system or service.
Recovery Point Objectives	refers to the point to which information used by Solution and/or the Services must be restored following a Disaster (eg: a cyberattack, natural

disaster, communications failure etc) to enable the activity to operate on resumption. This period shall be of 15 minutes.

Recovery Time Objectives	refers to the period of time following a Disaster (eg: a cyberattack, natural disaster, communications failure etc) within which the Solution and/or Services must be resumed or resources recovered. This period shall be of 2 hours.
Services	refers to a discrete unit of functionality provided to the Customer. example of Service includes amongst others software application, specialised IT Resources and Cloud computing resources such as Software as a Service (SaaS).
Solution	refers to the whole information system which will be managed by a third party. Solution can either be hosted at the Customer Data Centre or Third-Party Data Centre.

02. Principles of Security

- a) The Contractor acknowledges that the Customer places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Location and the security for the Solution or Service. The Contractor also acknowledges the confidentiality of Customer Data.
- b) The Contractor shall be responsible for the security of the Solution or Service and shall at all times provide a level of security which:
 - i. is in accordance with Best Industry Practice and Law; and
 - ii. meets any specific security threats to the Solution.
- c) The Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to the satisfaction of the Customer):
 - i. loss of integrity of Customer Data;
 - ii. loss of confidentiality of Customer Data;
 - iii. unauthorised access to, use of, or interference with Customer Data by any person or organisation;
 - iv. unauthorised access to network elements, buildings and tools used by the Contractor in the provision of the Services;
 - v. use of the Solution or Services by any third party in order to gain unauthorised access to any computer resource or Customer Data; and
 - vi. loss of availability of Customer Data due to any failure or compromise of the Services.

03. Security Requirements

The Contractor shall have the following responsibilities.

The Contractor shall abide by the provisions of the GMICT Information Security Policy available at <https://mita.gov.mt/en/GMICT/Pages/GMICT-Policies.aspx>.

In case of Supply of Equipment and Maintenance and Support Services the obligations of the Contractor shall be limited to Customer Data residing on the Hardware that is supported and maintained by the Contractor and/or Customer Data to which the Contractor may otherwise have access to whether directly or indirectly in providing the Service.

03.1 General

- a) Safeguard the confidentiality of data and ensure that the integrity and availability of the data that the Contractor manages and/or is responsible for by virtue of the Agreement is not

compromised.

- b) Ensure that it does not carry out and procure that its employees and subcontractors shall not carry out any act or omission which has or could reasonably be expected to have an adverse impact on the security of the Solution or Service and the Customer's business, activities, customers or systems.
- c) Protect the integrity of the Solution or Service or and any data and/or information processed by the Solution or Service during the provision of the Contract.
- d) Ensure that features used for the provision of the Solution or Service that are either not required for the business operation or which may pose a security risk are disabled or re-configured to minimize the associated risk. Upon request by the Customer, the Contractor shall issue a report showing the measures taken to harden the Service. The Customer reserves the right to undertake periodic reviews to assess the security status of the Service and to ask any rectifications thereof, which shall be carried out by the Contractor at no additional cost.
- e) If applicable, ensure that resources external to the Solution or Service used for the provision of the Solution or Service are accessed through Adapters. Upon request by the Customer, the Contractor shall provide a report listing the resources outside the Solution or Service that are being accessed by the Solution or Service and the tools being used for such access.
- f) Review and keep updated all security requirements indicated in this Schedule.
- g) Immediately notify the Customer of any security breach of any one of the security requirements listed in this Schedule that the Contractor becomes aware of.
- h) Pursuant to the circumstances referred to in the preceding clause:
 - i. take all reasonable steps necessary to remedy the breach or protect the Solution or Service against any such potential or attempted breach or threat to prevent an equivalent breach in the future. The Customer reserves the right to make recommendations on the necessary steps to be taken. In case of changes required by the Customer that are not reasonably covered by the obligations of the Contractor under the Contract, the parties shall agree in writing.
 - ii. as soon as reasonably practicable, provide the Customer with the full details (using such reporting mechanism as specified by the Customer from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.
- i) The Customer reserves the right to install further information security tools on the Solution to enhance the Protection, Detection and Response of such systems.

03.2 Information Security Policy

- a) The Contractor shall possess an Information Security Policy which:
 - i. Is endorsed by senior management;
 - ii. Is communicated to all the organisation's employees and relevant external parties;
 - iii. Is reviewed at planned intervals or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness;
 - iv. Affirms management's commitment and sets out the organisation's approach to managing information security;
 - v. Highlights the security policies, principles, standards, and compliance requirements of the organisation;
 - vi. Highlights responsibilities of the organisation's senior management and employees vis-a-vis information security; and
 - vii. Highlights the organisation's approach towards protecting the confidentiality, integrity and availability of information it manages/operates/comes into contact with.

03.3 Security of Customer Data

- a) Ensure that Customer data shall not be stored outside the Solution, if applicable, without the Customer's prior approval. Where the Customer provides approval, any transition of Customer Data outside the Solution shall be carried out using a communication method which commensurate with the classification of the data, as identified by the Customer. Furthermore, the storage of any personal data shall be in line with the Data Processing Agreement.

03.4 Risk Management

- a) The Contractor shall have a risk management program including policy and procedures for identifying, assessing, and mitigating risks.

03.5 Security in Third Party Agreements

- a) Procure from its sub-contractors involved in the provision of the Solution or Service under the Agreement an undertaking to be bound by the same terms and conditions of the Agreement, including but not limited to the security requirements set out in this Schedule. This Clause shall be without prejudice to the responsibility of the Contractor to provide the Service or Solution under this Agreement.
- b) Sub-Contractors personnel involved in the provision of the Solution or Service shall always be involved in continuous awareness sessions related to the content listed within this Schedule, provided by the Customer.

03.6 Asset Management

- a) Ensure that assets relevant in the lifecycle of information are identified and their importance is documented in an inventory. The lifecycle of information shall include creation, modification, processing, storage, transmission, deletion and destruction. Examples of relevant assets include:
 - i. Primary Assets
 - o Business process and activities for example processes that are necessary for the organisation to comply with contractual, legal or regulatory requirements;
 - o Information, for example personal information
 - ii. Secondary Assets
 - o Hardware such as data processing equipment, fixed equipment (servers etc)
 - o Software such as the operating system, service, maintenance or administration software;
 - o Network such as communication interfaces;
 - o Personnel such as users;
 - o Site such as premises or communication (eg: PABX etc)
 - o Organisation's structure such as subcontractors, suppliers, authorities etc.
- b) Ensure that the asset inventory is accurate, up to date, consistent and aligned with other inventories, where applicable.
- c) Return all Customer-owned assets within a contractually established period upon termination of employees and/or expiration of the Agreement.
- d) Protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, regulatory, contractual and business requirements. Examples of records are logs and/or reports created by information systems, asset inventories etc.
- e) Apply disposal controls for the secure disposal or reuse of resources. Such controls are

applicable to all media irrespective of warranty and including damaged equipment. Such controls shall be commensurate with the sensitivity of the data, as identified by the Customer. Verify all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

- f) For the purposes of secure disposal or re-use, equipment containing storage media that might possibly contain personally identifiable information (PII) shall be treated as though it does.
- g) Ensure that architectural diagrams of the provisioned Solution are created, maintained and provided to the Customer when required.
- h) With reference to cloud assets (i.e. a resource or policy configured or deployed onto a cloud-based environment) hosted on the Customer's cloud services, the Customer inventory shall account for information and assets stored on the cloud computing environment at the resource group level. The Contractor shall then be responsible for the upkeep of an inventory of data residing within the respective resource groups that they are responsible for.

03.7 Human Resource Security

- a) Return upon expiry or termination of the Agreement any credentials, keys, tokens and other similar devices required/used for the provision of the Service pursuant to the Agreement. Return the same in relation to Contractor Personnel that cease to provide a service on the Agreement.
- b) Ensure that access rights granted to Contractor Personnel are removed upon expiry or termination of the Contract or otherwise upon in relation to such Contractor Personnel that have been replaced.

03.8 Information Security Awareness and Training

- a) Provide training on a continuous basis to Contractor Personnel involved in the provision of the Services in relation to the security requirements listed in this Schedule, including training on security awareness. The Contractor shall also ensure that it provides Contractor Personnel with access to documented operating procedures detailing the process carried out by the Contractor pursuant to the Agreement.

03.9 Physical and Environmental Security

- a) Ensure that physical controls are in place to prevent unauthorised access to Contractor premises.
- b) Ensure that Customer Data are stored in a secure manner and physically protected from unauthorised access and damage. Personal data shall be stored in accordance with the Data Processing Agreement.
- c) Ensure that media containing information is protected against unauthorized access, misuse or corruption during physical transportation.
- d) Ensure that equipment, information or software is not taken off-site without the prior authorization of the Customer. Such an authorization shall be commensurate with the sensitivity of the respective data, as identified by the Customer.
- e) Apply security to off-site assets (i.e. assets not located within premises managed by the Customer) taking into account the different risks involved.
- f) Maintain a record for incoming and outgoing physical media, whenever physical media are used for information transfer containing personally identifiable information (PII). This record shall include the type of physical media, the authorized sender / recipients, the date and time, and the number of physical media.

- g) Ensure that personally identifiable information on media leaving the Contractor's or the Customer's premises is authorized by the Customer and is not accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

03.10 Change Management

- a) Ensure that changes to the Solution are carried out in a controlled manner through planning and testing of changes and assessment of potential impacts. The Contractor shall maintain a record of the changes.

03.11 Separation of Development and Operational Facilities

- a) If applicable, maintain development, operational and test environments separate to reduce risks of unauthorised access or changes.

03.12 Capacity Management and Information Back-up

- a) If applicable, monitor back-ups, capacity and performance regularly for the Solutions used for the provision of the Service or Solution.
- b) Ensure that backups of production data are backed up according to an established backup schedule as agreed by the Customer.
- c) Ensure that data backups are stored as required by the Customer and shall be made available when requested by the Customer.

03.13 Protection from Malware

- a) Set up protective mechanisms to ensure that the Solution used for the provision of the Services, including any patches, updates or upgrades provided through any electronic media by the Contractor do not include harmful electronic data (including malicious code) which causes, or is likely to cause, detriment or failure or loss of performance, or loss of service, or harm in any degree to any computer systems or network systems owned by the Customer or other Third Parties.
- b) Ensure that Solution used for the provision of the Services shall be patched regularly, installed with the latest updated version of end-point security software and no end of support/legacy software shall be left on the Solution, unless mitigating controls are in place.
- c) The Contractor shall also implement lockout mechanisms on such Contractor equipment and regulate the use of Contractor equipment (including laptops) outside Contractor premises.
- d) Ensure that operating systems are hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.
- e) Implement detection, prevention and recovery controls to protect against malware, combined with appropriate user awareness.

03.14 Exchange of Information

- a) Set-up and maintain information handling procedures to ensure that the method chosen to exchange communications is commensurate with the sensitivity of the information exchanged, as identified by the Customer. For such purpose the Contractor shall have mechanisms in place to send and/or receive encrypted emails, to manage portable devices securely and to deliver sealed envelopes by hand rather than by post, amongst others.

03.15 Clock Synchronisation

- a) Ensure that clocks are synchronized with an accurate time-source.

03.16 Access Control

- a) Ensure that the Contractor Personnel accessing the Solution are granted minimum rights and privileges required to execute their duties, as per least privilege principle. The Contractor shall also ensure that when in use, the Solution is not connected to the Internet whilst accessing the Solution, unless as agreed to with the Customer.
- b) Ensure that access rights on the Contractor equipment and/or any Information System used for the provision of the Services are granted according to the 'least-privilege-required' principle. For such purpose, the Contractor shall enable audit logs to monitor and review access rights regularly. The Contractor shall also undertake to immediately disable user-accounts of Contractor Personnel that cease to provide a service on the Agreement.
- c) Ensure that access rights on the Solution providing the Service (software application and database) are granted according to the 'least-privilege-required' principle and as authorised by the Customer. For such purpose, the Contractor shall set-up and maintain a formal process for granting, changing or revoking access rights.
- d) Ensure that access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall 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.

03.17 Account Management

- a) The Contractor shall not use generic accounts, unless with the prior written approval of the Customer. Named accounts shall be assigned to individual personnel. If more than one individual has access to stored information, then they shall each have a distinct account for identification, authentication and authorization purposes.
- b) In case of use of generic accounts by the Contractor to operate and manage the Service, as approved by the Customer, provide the Customer with the procedure the Contractor shall use to handle, store, access and change passwords. The Customer shall review the details submitted and may request the Contractor to revise such procedures to ensure an effective way of securing passwords.
- c) Ensure that an account is not transferred from one person to another.
- d) Ensure that disabled or deleted accounts are not assigned to other individuals.
- e) Ensure that Multi-Factor Authentication is enabled for Contractor Personnel Accounts
- f) Provide, upon request by the Customer, a report listing all accounts associated with the Contractor Personnel including their status (active, inactive or deleted) and the reason for such status (e.g. in the case of a deleted account due to Contractor Personnel that ceased to be involved in the provision of the Service).
- g) Administer, manage and maintain end-user accounts pertaining to the related services (where applicable), including but not limited to operating system, services, application and database user accounts.
- h) Adopt a 'least privilege principle' approach throughout the management and use of accounts unless specific circumstances mandate otherwise. In the case of specific circumstances, the Contractor shall substantiate the reasons thereof.

- i) The Contractor shall ensure that an account is deleted as soon as an employee is no longer working with Service Provider.

03.18 Passwords

- a) Passwords used on all Solution should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers.
- b) Implement measures to safeguard against the sharing of passwords between Contractor personnel and implement controls to safeguard the confidentiality of passwords stored in a password management system.
- c) Ensure that all personal computers utilised by the Contractor personnel are password protected to prevent unauthorised access.
- d) For Business Critical Solutions, or as directed by the Customer,
 - i) A copy of non-interactive accounts used by the Contractor are to be stored within the Customer's credential management solution;
 - ii) The interactive business continuity and disaster recovery (break-glass) accounts and passwords are to be solely stored within the Customer's credential management solution and accessed by the Contractor solely after obtaining approval from the Customer, providing a justification;
 - iii) The interactive highly privileged (super-user) account and password is to be solely stored within the Customer's privileged credential management solution and accessed by the Contractor solely after obtaining approval from the Customer, providing a justification.

03.19 Clear-desk and clear screen

- a) Ensure that papers and storage media containing Customer Data are stored in a secure manner (e.g. in locked cabinets) when not in use to reduce risks of unauthorised access, loss or damage to the Customer data.

03.20 Connecting to MAGNET

- a) In the event that the Contractor requires remote access to the Solution network connectivity shall be provided through a Virtual Private Network (VPN) using strong two factor authentication. The VPN solution may be provided by the Customer or otherwise provided by the Contractor as part of the provision of the Solution. Where the VPN solution is to be provided by the Contractor the VPN solution shall be approved by MITA, in order to safeguard the integrity of its network.
- b) MITA reserves the right to disconnect the system from MAGNET, if it is determined that the system is posing a security risk on the underlying infrastructure.

03.21 Teleworking

- a) Ensure that in cases where Contractor Personnel work outside Contractor premises appropriate security measures are implemented.

03.22 Protection of Production data

- a) Ensure that test data is used for testing purposes. Where test data cannot be used, the Contractor shall with the prior approval of the Customer use live data that is sanitised or, only where strictly necessary, use live data on a test environment that shall have the same level of security controls as in the operational environment. The Contractor shall delete any live data

once testing is completed and shall inform the Customer in writing of such deletion for audit trail purposes.

- b) Where applicable, segregate production and non-production environments to prevent unauthorized access or changes to information assets.

03.23 Operational Procedures and Responsibilities

- a) Ensure that data, including temporary data, is retained as per the retention period established and communicated by the Customer.

03.24 Control of technical vulnerabilities

- a) Implement measures to detect and manage technical vulnerabilities in the Solution in order to reduce risk from exploitation of technical vulnerabilities.

03.25 Information Security Incident and weakness management

- a) Set-up and maintain procedures to monitor, report and manage security incidents and security weaknesses.
- b) Provide accurate information in a timely manner in the case of an investigation or security breach.
- c) Note and report to the Customer any observed or suspected information security weaknesses in systems or services governed through this Agreement.

03.26 Hardening

1. Ensure that devices are configured according to industry and security baselines and as requested by the Customer.
2. Ensure that servers are configured according to industry and security baselines, have installed the latest version update of the end-point-security software and to regulate network traffic to and from servers according to the 'least-privilege' principle.
3. Ensure traceability by enabling operating system security audit logs on servers.
4. Implement database hardening mechanisms to safeguard sensitive fields/records within the database.

03.27 Audit Logging and Protection of Log Information:

- a) Ensure that audit logs are enabled on the Solution and that access to modify audit logs is restricted. The Contractor shall also ensure the capability of creating a secure audit record each time a user accesses, creates, updates, archives or deletes information via the system. Such audit logs shall uniquely identify the user, function performed and date and time the function was performed. Where possible, event logs shall record whether or not personally identifiable information (PII) has been changed (added, modified or deleted) as a result of an event and by whom.
- b) Store logs in native format and upon the request of the Customer, provide the Customer with the security logs. The Customer may request a soft copy of the security logs, for which the Contractor shall be obliged to provide the tool that enables the Customer to read such logs without requiring access to the Solution.

- c) Ensure that changes to the data processed by the Solution are recorded and stored to keep track of the changes (retain former version), the user that carried out the change and the date and time when the data was changed.
- d) Maintain audit logs for a period, as identified by the Customer, to assist in future investigations. As a minimum, database audit logs shall be retained (either online or offline) for the duration of the Agreement and the Contractor shall not delete/modify any of the audit logs prior to relinquishing the environment upon expiry or termination of the Agreement in accordance with its terms. The Contractor shall, unless it proves that it is not technically feasible, retain all other logs until such time as the Customer specifies otherwise.
- e) Enable database audit logs on the database, in particular, to meet the data protection requirements in as detailed in the Data Processing Agreement.
- f) Enable the copying of audit data to the Customer's Security Information and Event Management (SIEM) tool, in instances where this is requested by the Customer.
- g) Audit logs as configured by the Customer shall not be modified unless approved by the Customer.

03.28 Information Security Reviews

- a) Regularly review information systems for compliance with:
 - i. the Contractor's Information Security Policy
 - ii. the GMICT Information Security Policy
 - iii. the provisions of this Security Schedule
- b) The Customer shall carefully plan and agree on such audit activities with the Contractor to minimise disruptions to business processes.
- c) The Customer reserves the right to carry out security assessments. The Contractor shall fully collaborate with the Customer in such security assessments and carry out any necessary remedial measures in order to protect the Customer's infrastructure in a timely manner. Failure to implement the necessary remedial measures upon the agreed timeframes shall be treated as a serious misconduct.
- d) The Customer reserves the right to implement the necessary security controls to detect and manage security events on the Solution in order to protect the Customer's infrastructure. The Contractor is expected to fully cooperate with the Customer in this regard.

03.29 Acceptable Use

- a) Ensure that the installation and use of utility programs that might be capable of overriding systems and application controls are restricted and tightly controlled. The Contractor shall ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorised personnel, and that the use of such programs is reviewed and audited regularly.

03.30 Cloud Environment

- a) The Contractor shall ensure the integrity of all virtual machine images and resources with the resource group at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state.

03.31 Business Continuity Management, including Disaster Recovery

- a) Implement redundancy mechanisms on the Solution as requested by the Customer for business continuity purposes and perform regular checks to ensure that redundancy mechanisms are working as expected. The redundancy mechanisms should take into consideration the Recovery Time Objectives and Recovery Point Objectives as set out in this Contract.
- b) Develop and maintain, throughout the term of the Agreement, appropriate business continuity and/or disaster recovery plans in relation to the Solution that cater for all instances where the Solution is affected, irrespective of whether the problem rests with the Solution or arises from external resources. The plan shall identify any Customer responsibilities and the Contractor shall liaise with the Customer accordingly on such aspects. The plans should take into consideration the Recovery Time Objectives and Recovery Point Objectives as set out in this Contract.
- c) Provide a copy of the business continuity and/or disaster recovery plans to the Customer.
- d) Test the business continuity and/or disaster recovery plans on a regular basis and highlight any lessons learnt and further improvements that should be taken into consideration.

03.32 Correct Processing in Software Applications

- a) Determine domain specific security controls required for the correct processing by the application and apply as required.
- b) Ensure that appropriate controls are designed as part of the software application, including user developed applications to ensure correct processing (including storage, transmission, retrieval and access) of data. The controls shall include validation of input data, internal processing and output data and shall also take into account security vulnerabilities. The software application shall support session-timeout after a defined period of inactivity.
- c) Ensure that appropriate security controls are implemented as an integral part of the Solution to safeguard the confidentiality, integrity and availability of the data processed or stored by the Solution.
- d) Implement measures to provide assurance that all changes directly correspond to a registered change request, as per agreed service level agreements.
- e) Protect information passing over public and internal networks from fraudulent activity, contract dispute and unauthorized disclosure and modification.
- f) Protect information involved in application service transactions to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
- g) The following concepts shall be considered when designing a Solution:
 - i. **Least Privilege** – The software should operate only when necessary and with minimum level of access rights (privileges) given explicitly to it for a minimum of time to complete the operation. The design of software engineering practices should be highly cohesive and loosely coupled at the same time.
 - ii. **Separation of Duties (or Compartmentalization Principle)** – Completion of a single task (both in terms of software and people roles) is dependent upon compartmentalized two or more conditions, all of which need to be satisfied before an operation can be completed.

- iii. **Defense in Depth** – Single points of complete compromise should be eliminated or mitigated through the incorporation of a series or multiple layers of security to safeguard the data processed by the Solution.
- iv. **Fail Secure** – Aimed to maintaining confidentiality, integrity and availability by defaulting to a secure state and rapid recovery of software resiliency upon design or implementation failure.
- v. **Economy of Mechanisms** – This refers to the ‘Keep It Simple’ principle because the likelihood of a greater number of vulnerabilities increases with the complexity of the software architectural design and code. By keeping the software design and implementation details simple, the attack surface of the software is reduced:
 - a. Unnecessary functionality or unneeded security mechanisms should be avoided
 - b. Strive for simplicity
 - c. Strive for operational ease of use
- vi. **Complete Mediation** – Ensures that authority is not circumvented in subsequent requests of an object by a subject, checking for authorization (rights and privileges) upon every request for the object. The access requests by a subject for an object is completely mediated each time, every time.
- vii. **Open Design** – Security through obscurity should not be the sole and primary security mechanism in the software. The design should take into account the need to leave the design open but keep the implementation of the protection mechanisms independent of the design.
- viii. **Least Common Mechanisms** – Sharing of mechanisms that are common to more than one user or process at different levels of privilege should not be permitted. Design should isolate the functions by levels of privilege.
- ix. **Psychological Acceptability** – Security mechanisms should be designed to maximize usage, adoption, and automatic application. Security protection mechanism should be easy to use, does not affect accessibility and is transparent to the user.
- x. **Weakest Link** –The resiliency of software against hacker attempts will depend heavily on the protection of its weakest components, be it the code, service or an interface.
- xi. **Leveraging Existing Components** – This is a security principle that focuses on ensuring that the attack surface is not increased, and no new vulnerabilities are introduced by promoting the reuse of existing software components, code and functionality.

The use of a single Data Access Layer (DAL) to mediate all access to the backend data stores supports the principle of leveraging existing components. Therefore, it is advisable from a security standpoint, that the software functionality is broken down into tier architecture - presentation, business, and data access tiers.

- xii. **Accountability (Logging/Auditing)** – Audit fields of categorised information that was changed must be logged for all administrative (privilege) or critical transactions as defined by the business. The information should address the deniability of actions taken by either a user or the software on behalf of the user. Audit logs must be appended to and never to overwrite older logs.

Bare minimum audit fields should be the following:

- i. Who – the subject which may be a user or a process
- ii. Did What – Operations such as C.R.U.D
- iii. Where – the object on which the operation is performed such as a file or table
- iv. When – Timestamp of the operation
- v. Before and after snapshot of the information

- h) In the case that the software requires the use of secret keys to integrate or communicate within the same, related or third-party components, the keys must be stored only in the Customer's password managed solution or in an alternative solution that is approved by the Customer.
- i) Review and test business critical applications as determined by the Customer when operating platforms are changed to ensure there is no adverse impact on the Customer's organizational operations or security.
- j) Establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
- k) Perform testing of security functionality during development. New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.
- l) The Contractor shall carry out the following security testing during the testing phase of the lifecycle prior Go Live Date:
 - i. Perform security testing to at least verify the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls.
 - ii. Implement encryption controls that make use of sufficient strength routine to withstand brute force attack against the encryption routine.
 - iii. Perform randomisation or fuzzing techniques to cover the main input parameters.
 - iv. Perform denial of service and stress testing specifically designed to test the application resources.
 - v. Perform an automated security vulnerability scan using static code analysis methodology. The tool used shall as a minimum scan against the current OWASP Top Ten Security Vulnerabilities (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
 - vi. The Contractor shall immediately inform the Customer if security vulnerabilities result from the scan. The Contractor shall draw up a treatment plan to address these vulnerabilities. The Solution will not be deployed on the live environment unless security vulnerabilities have been properly addressed. The Contractor shall provide a copy of the scan results evidencing that these security vulnerabilities have been rectified to the Customer. The reports submitted by the Contractor to the Customer (relevant to the security vulnerability scan) shall also indicate the name of the tool used to carry out the security vulnerability scan.
 - vii. When using third-party dependencies / components, the Contractor shall scan for vulnerabilities using an automated Software Composition Analysis mechanism. The vulnerabilities identified shall be treated as above.
- m) Implement data input and output integrity routines (i.e reconciliation and edit checks) for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
- n) Use secure and encrypted communication channels when migrating physical servers, applications, or data to virtualized environments and, where possible, use a network segregated from production-level networks for such migrations.
- o) The Customer reserves the right to audit developments processes and controls implemented by the Contractor.
- p) The Customer may carry out scanning for security vulnerabilities itself before or after the implementation. The Customer shall inform the Contractor of any security vulnerabilities identified, and the Contractor shall ensure that these are rectified either before go-live or within the service levels. (if the scan is carried out after the go-live date).

03.32.1 Additional Requirements for Web Applications and APIs (where applicable) prior Go Live Date

- a) The Contractor shall carry out an automated security vulnerability scan using dynamic code analysis methodology. The tool used shall as a minimum scan against the current OWASP Top 10 Web Application Security Risks and OWASP API Security Top 10:
 - a. <https://owasp.org/www-project-api-security/>
 - b. <https://owasp.org/www-project-top-ten/>
- b) A content security policy (CSP) should be defined to restrict the resources to be loaded in the browser.
- c) A web-facing application shall be segregated from the database. Access between the application and database shall be bound to the least access privilege principle.

03.33 Governance

- a) The Customer may carry out periodic checks/assessment to ensure that the Contractor is performing its responsibilities as set out in this Schedule.
- d) In such event, the Contractor shall ensure that its personnel, subcontractors or agents provide its procedures relative to the operation, administration and management of all the components, as well as copies of all documentation requested by the Customer, relating to the preparation, conduct and results of the verification, validation, quality control and quality assurance processes carried out on the Solution/Service, where applicable.
- e) If, as a result of an audit, the Customer considers that any activity or omission by the Contractor has or could reasonably be expected to have an adverse impact on the Solution/Service, Customer's business, activities, customers or systems, the Customer shall inform the Contractor of the actual or potential adverse impact. The Contractor shall immediately take all the necessary measures to rectify the situation within the shortest possible timeframes to be agreed upon between the Customer and the Contractor.
- f) If the Contractor fails to take the necessary measures in the agreed timeframe, the Customer shall have the right to suspend access to the external resources and take any additional remedial measures to isolate the Contractor's environment. The Customer shall consider this failure on the part of the Contractor as serious misconduct.