Technical and Organisational Measures to Ensure the Security of Personal Data

Description of the technical and organisational measures implemented by the vendors(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data

- The appropriate cryptographic controls shall be applied to protect information assets which require stringent security. Examples of cryptographic controls are public and private key cryptosystems. Vendor(s) shall define and deploy the procedures for maintenance of the keys.

- Wherever required, the appropriate encryption controls shall be implemented by the Vendor(s) to protect the confidentiality and integrity of information on the applications/ systems that are used to provide services to the Emeritus Group. The encryption type and other implementation details shall be decided by the Vendor(s) after considering relevant legislative and regulatory requirements.

- The access to sensitive commands pertaining to encryption key data on the telecom switches shall be restricted to key administrators only. The activities of the users having access to such sensitive commands shall be appropriately logged and monitored periodically.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Important information assets shall be assigned an asset criticality rating as per guidelines laid down in the Asset Management Procedure, to assess the relative importance of such assets to Emeritus Group and to determine the level of security measures to be implemented for their protection.

- All information assets are required to be labelled by the Vendor(s) and maintained as per a formal Information Labelling and Handling Guideline. These assets shall be labelled (marked) using the classification scheme only to indicate the level of sensitivity of the information. This may exclude public information.

- The Vendor(s) is required to ensure that they consider appropriate automated controls while designing the information systems that are used to provide services to Emeritus Group.

- All new application systems developed/to be deployed by the Vendor(s) to provide services to Emeritus Group shall be formally reviewed for compliance with the security policy before being deployed in the production environment. The development, testing, operations, and maintenance teams of the Vendor(s) shall be trained on security aspects of application development and maintenance.

- System requirements specification shall include controls in the application for the input data provided. Periodic reviews of the content of key fields or data files to confirm their validity and

integrity shall be conducted by the Vendor(s). Procedures for responding to validation errors and defining the responsibilities of personnel involved in the data input process shall be documented by the Vendor(s).

- Risk associated to processing facilities shall be minimised by considering security controls in the design and implementation phase of applications development and deployment. Specific security controls that are required to be incorporated in this stage are as follows:

    a. Session or batch controls, to reconcile data file balances after transaction updates.

    b. Balancing controls, to check opening balances against previous closing balances, namely:

        i. Run-to-run controls.

        ii. File update totals.

        iii. Program-to-program controls.

    c. Validation of system-generated input data.

    d. Checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers.

    e. Hash totals of records and files.

    f. Checks to ensure that application programs are run at the correct time.

    g. Checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved.

    h. Creating a log of the activities involved in the processing.

- The validity of the message integrity shall be protected by appropriate encryption management for developing applications that will be used to provide services to Emeritus Group. It deals with methods that ensure that the contents of a message have not been tampered and/ or altered. Message integrity protection requirements shall be identified by Vendor(s) in the applications and information systems and the controls for integrity shall be implemented. An assessment of security risks shall be carried out by Vendor(s) to determine if message integrity is required. Appropriate method of message integrity check shall be identified as per the risk assessment results.

- During the development stage of application systems, data generated from the application system after processing of the stored information shall be validated to ensure that output is correct and appropriate.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Vendor(s) shall ensure that they have an incident management team in place to respond to information security incidents pertaining to information asset of Emeritus Group. This team shall submit security incidents reports to Emeritus Group on request.

- A formal Information Security Incident Management Process shall be developed and implemented within Vendor(s) organisation. The process shall include the incident reporting, incident response, escalation, and incident resolution pertinent to Emeritus Group information. The Vendor(s) employees shall be made aware of their responsibilities regarding information security incident management.

- All employees of Vendor(s) shall report the information security weaknesses to their Incident Management Team. The users shall not attempt to prove the suspected security weaknesses. In addition to this, users shall not test the existence of vulnerability in any information system used to provide services to Emeritus Group.

- The responsibilities shall be identified and defined within Vendor(s) organisation to ensure a quick, efficient, and systematic response to information security incident. The procedures shall be established to handle the different types of information security incidents.

- A formal review process shall be conducted after the recovery from incident has been completed (within two weeks). A feedback mechanism shall be available to identify improvements to the incident handling process.

- Vendor(s) shall ensure that there are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

- The audit trails and similar evidence shall be collected during the whole incident handling process - from the initial incident report to the incident follow-up. The audit trails shall be used for the following:

    a. Internal problem analysis (or root cause analysis) of how the incident occurred.

    b. As forensic evidence in relation to a potential contract breach or regulatory requirement or in the event of civil or criminal proceedings and shall include the following types of logs:

        i. Communication log.

        ii. Incident survey, containment land eradication logs; and

        iii. Raw data, as in. actual system logs.

    c. Retention of incident reports and logs shall be in accordance with the legal and regulatory requirements; and

d. The incident handling procedures shall be regularly reviewed and tested to establish their ongoing effectiveness.

- Vendor(s) shall ensure that the evidence is collected in a manner that does not destroy its evidentiary value. While collecting the evidence, the following shall be considered by Vendor(s):

    a. Applicability of evidence: The evidence can be used in court; and

    b. Weightage of evidence: The quality and completeness of the evidence.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- All technical vulnerabilities of information systems that are used to provide services to Emeritus Group shall be identified and documented. Appropriate measures shall be taken to address the associated risk.

- Timelines shall be defined to respond to technical vulnerabilities observed in the system. Vendor(s) shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, and any coordination responsibilities required.

- All patch management shall be followed using a formal Patch Management Process.

Measures for user identification and authorisation

- Access control rules and rights for each user or group of users shall be clearly stated. Access controls are both logical and physical, and these shall be considered together to prevent any unauthorised access to information assets that are used to provide services to Emeritus Group.

- Procedures for user registration and de-registration are required to be defined, documented, and implemented for granting access to information systems that are used to provide services to Emeritus Group. These procedures shall include the following:

    a. All users shall have a unique user ID based on a standard naming convention, for accessing information systems.

    b. Appropriate authorisation shall be obtained prior to creating the user IDs.

    c. An audit trail shall be kept for all requests for addition, modification or deletion of user accounts/ IDs and access rights.

    d. User accounts shall be reviewed at regular intervals, at least quarterly for sensitive systems and half-yearly for the other systems, to identify and facilitate removal/ deactivation of inactive accounts or accounts that have not been used for a long duration.

    e. The Application Administrator must be responsible for implementing access control as defined by the Application owner.

f. The results of user account reviews, including subsequent actions, shall be documented to provide an audit trail; and

g. "Guest" accounts and other default accounts shipped with software/ applications shall be disabled or their passwords changed from the default value in case there is a justified business requirement for using these accounts.

- Privilege accounts have administrator access on the system. The creation and allocation of privilege user accounts/IDs on information systems that are used to provide services to Emeritus Group shall be controlled through a formal authorisation process. The authorisation process shall consider the following:

    a. The privilege associated with each system (e.g., operating systems, databases, applications etc.) and their corresponding users are identified.

    b. The privileges are allocated to individuals on a 'need-to-have' basis. The authorisation process for access

    c. Vendor(s) shall approve the usage of group privilege user ids if required. Accountability shall be ensured for group privilege user IDs that are used to access information of Emeritus Group.

- Passwords shall be distributed to the users in a secure manner. The following controls relating to password management should be implemented:

    a. Users should be forced to change their password during the first log-on and after 45 days of each password change. However, users shall receive password change warning 15 days prior to its expiry.

    b. Passwords should have combination of alpha-numeric characters and a minimum length of eight characters.

    c. Passwords should have a minimum age of one day.

    d. Passwords for all user and privilege accounts should expire after 45 days from its last change, except for accounts used by services; password for privilege accounts should have lesser period to change the password

    e. A record of five previous passwords should be maintained to prevent the re-use of these passwords.

    f. A maximum of three successive login failures should result in account lockout.

    g. A 'locked out' user should not be able to login until the account is unlocked by the system administrator or by the user himself, using the 'Password Reset' solution.

    h. Passwords should not be displayed in clear text when it is being keyed in or otherwise.

i. Support procedures should be in place to deal with forgotten passwords and account lockouts.

j. User password resets should be performed only when requested by the individual to whom the user ID is assigned, after verification of their identity by a defined procedure.

k. When passwords are reset, users should be forced to change their password to a password of their choice on the first use after the reset.

l. Default accounts should be disabled and/or the associated default passwords shall be changed immediately.

m. A secure 'Password List' should be maintained for all critical accounts. Only authorised individuals should have access to this 'Password List'; and

n. Passwords should not be coded into logon scripts, batch programs or any other executable files when user authentication or authorisation is required to complete a function.

- The review of access rights shall consider the following:

  a. User access rights are reviewed at regular intervals, for e.g., a period of three months and after any change in status of employment, such as promotion, demotion, or termination.

  b. Whenever the user is moving from one employment to another within the Vendor(s)'s organisation, user access rights are to be reviewed and re-allocated.

  c. Authorisations for special privileged access rights are reviewed at more frequent intervals, for e.g., every month.

  d. Privilege allocations are checked at regular intervals to ensure that unauthorised privileges have not been obtained; and

  e. Changes to privileged accounts are logged for periodic reviews.

- The Vendor(s) shall ensure that users with access to information or information systems that are used to provide services to Emeritus Group shall be advised for the following:

  a. Keeping the passwords confidential and avoiding the recording of passwords unless this can be stored securely and the method of storing approved.

  b. Changing passwords whenever there is any indication of possible system or password compromise.

  c. Choosing quality password which is easy to remember but difficult to guess; and

  d. Changing passwords at regular intervals or based on the number of accesses (passwords for privileged accounts shall be changed more frequently than normal passwords).

Measures for the protection of data during transmission

- The Vendor(s) shall ensure that its users shall be provided with access to the services only on a 'need-to-have' basis. An authorisation process shall be developed and followed to ensure that only users who are authorised can access the respective network segments and services. These services are required to be reviewed at regular intervals.

- Virtual Local Area Networks (hereinafter referred to as VLAN) should be created to segregate the networks being used to provide services to Emeritus Group.

- The Vendor(s) shall ensure that:

    a. Remote access connections to networks being used to provide services to Emeritus Group are provided only to authorised users. This shall be authorised by Emeritus Group.

    b. Secure channels like Virtual Private Networks shall be implemented.

    c. Modems connected to the end user workstations/laptops are configured to reject all incoming traffic initiated from other external sources; and

    d. Only approved remote control software is used in the network for external connections, if required.

- Equipment identification shall be used, if it is important that the communication can only be initiated from a specific location or equipment. An identifier shall be used to indicate whether this equipment is permitted to be connected to the network used to provide services to Emeritus Group.

- The security of networks associated with information that belongs to Emeritus Group should be divided into separate physical and/ or logical network domains. A graduated set of controls shall be applied in different logical network domains to further segregate the network's security environments.

- The Vendor(s) shall ensure that they segregate the network used for Emeritus Group from the rest of its network.

- The Vendor(s) should ensure that the connection capability of users is restricted through firewalls. FTP downloads and uploads from the Internet shall be permitted only for business use and only after approval from Emeritus Group.

- Network routing controls are based on positive source and destination address-checking mechanisms. The Vendor(s) shall ensure that they implement network routing controls to prevent any unauthorised access to information systems that provide services to Emeritus Group.

Measures for the protection of data during storage

- The information of Emeritus Group which is managed by the Vendor(s) is required to be backed up in accordance with a Back-up Procedure. Restoration-testing is required to be conducted for the backed-up data at regular intervals as defined by Emeritus Group and logs for

backup/restoration shall be stored with restricted access. Log analysis shall be carried out for all failed backup and restorations and corrective actions shall be taken.

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

- The results of the monitoring activities are required to be reviewed at regular intervals by the Vendor(s). The intervals shall be decided as per criticality of the information systems and a consolidated report for all reviewed monitoring activities shall be prepared.

- An appropriate tool for storing and monitoring the logs shall be implemented by the Vendor(s). Log storing and monitoring shall cover the following:

    a. Authorised access.

    b. All privileged operations.

    c. Unauthorised access attempts; and

    d. Changes to, or attempts to change, system security settings and controls.

- The log information of systems/equipment/network devices used to provide services to Emeritus Group shall be protected against unauthorised access, alterations, and operational problems. The Vendor(s) shall ensure that access to logs shall be provided only on a 'need-to-know' and 'need-to-have' basis. Appropriate controls shall be implemented to prevent:

    a. Alterations to the message types that are recorded.

    b. Log files being edited or deleted; and

    c. Storage capacity of the logging media being exceeded.

- The information systems being used to provide services to Emeritus Group are required to be configured in such a way that the system administrator and system operator activities are logged and are secure from unauthorised modification. The system administrator and system operator shall not have rights to access administrator and operator logs. The logs shall be reviewed by an independent person to identify any malpractices happening.

- The Vendor(s) are required to maintain logs of all the faults related to the data processing problems and communication systems that are used to provide services to Emeritus Group. The Vendor(s) shall ensure that such issues are corrected as per the Service Level Agreement (hereinafter referred to as the SLA). The Vendor(s) shall also ensure that root-cause analysis is carried out to prevent any reoccurrence of faults.

Measures for ensuring system configuration, including default configuration

- Vendor(s) shall identify program librarians to maintain source libraries of operational application systems in configuration management database.

- All source codes shall be stored in a secure environment. All updates or issue of program sources to developers shall be carried out through an authorised request.

- Configuration changes to program source codes shall be made through configuration management process to prevent any unauthorised and unintentional changes.

- Previous versions of source programs shall be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.

- The technical compliance checking shall cover the penetration testing and vulnerability assessments of systems/ network devices that are used to provide services to Emeritus Group information. All identified vulnerabilities shall be analysed and fixed within a definite timeframe. Emeritus Group reserves the right to review the vulnerability closure report and / or conduct technical compliance checking on Vendor(s) network.

Measures for internal IT and IT security governance and management

- Procedures are required to be in place, to ensure that activities performed for day-to-day system operations are carried out in a secure manner. Vendor(s) is required to document all Operating Procedures to maintain confidentiality, integrity and availability of that specific platform or application.

- The Vendor(s) is required to ensure that procedures are made available to all their employees who are involved in the respective operations and processes for Emeritus Group.

- All system and application administrators shall ensure that operating procedures are kept up to date in accordance with any system changes.

- To ensure that the security of the systems/environments is not compromised, Vendor(s) is required to manage the change(s) in the production systems/environment of assets used to provide services to Emeritus Group.

- Vendor(s) shall ensure that:

    a. Change control is required to be applied to all security aspects of the production applications and infrastructure associated with Emeritus Group.

    b. All Vendor(s) service providers are required to manage the change(s) to the systems and services supplied to Emeritus Group.

    c. All approved changes are required to be tested in a test setup prior to implementing them on the production systems.

- Vendor(s) is required to apply the patches to the systems being used to provide services to Emeritus Group in a timely manner to ensure that the systems are running at their optimum level and the threat from vulnerabilities and malicious agents are reduced to an acceptable level.

- Vendor(s) is recommended to implement segregation of duties so that no one user can subvert any security control associated with Emeritus Group information. Any one employee of Vendor(s) should not be responsible for more than one of the following duties, at any given point of time: data entry, computer operation, network management, system administration, systems development, change management, security administration, security audit, security monitoring.

- Where segregation of duties is not possible or practical, the process is recommended to include compensating controls such as monitoring of activities, maintenance and review of audit trails and management supervision. Collusion shall be removed from the design and deployment architecture of the compensating control.

- The Vendor(s) is required to ensure that the capacity of systems used to provide services to Emeritus Group is monitored on a periodic basis. Capacity planning shall be carried out by the Vendor(s) to ensure future capacity requirements and enhancements. This is required for security-related logging, analysis and exception-reporting for the systems being used to provide services to Emeritus Group. The system/application administrator shall monitor capacity utilisation and project future capacity requirements to ensure that adequate processing power and storage are available for systems that are used to provide services to Emeritus Group.

- The acceptance criteria for new information systems, upgrades and new versions of system/software are required to be followed by the Vendor(s) for any new system that is deployed to provide services to Emeritus Group.

- While providing services to Emeritus Group, the Vendor(s) may outsource some services to a Sub-contractor. When using the services of a Sub-contractor, the Vendor(s) shall ensure that agreed service delivery levels are met and security controls are adhered to by the Sub-contractor. The Vendor(s) shall monitor and review the services of its sub-contractor on an ongoing basis to ensure that services offered to Emeritus Group are supported without any interruption.

Measures for certification/assurance of processes and products

- A list of all relevant statutory, regulatory, and contractual requirements shall be maintained by Vendor(s).

- Vendor(s) shall ensure the following:

    a. Acquiring software only through reputable sources.

    b. Maintaining proof of ownership of licenses of software procured to provide services to Emeritus Group; and

    c. Carrying out checks that only authorised and licensed software are used to provide services to Emeritus Group.

    d. Emeritus Group reserves the right to audit the Vendor(s) for all / any authorised and/or licensed software used to provide services to Emeritus Group.

Measures for ensuring data minimisation

- A data protection and privacy policy shall be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information of Emeritus Group's customers. Vendor(s) shall ensure that they adhere to the information privacy policy for protecting personal information of Emeritus Group's customers.

- Vendor(s) shall ensure that their users are prevented from misusing the information processing systems/ facility that is used to provide services to Emeritus Group. Adequate detection and monitoring controls shall be implemented to prevent any misuse on the information systems/ facilities.

- The audit activities involving checks on operational systems shall be carefully planned as they may result in service disruption and in turn affect the services for Emeritus Group. Vendor(s) shall ensure checks shall only allow read-only access.

Measures for ensuring limited data retention

- The mechanism used for the storage and handling of records pertinent to Emeritus Group, shall ensure clear identification of records and the retention period as defined by national or regional legislation or regulations.

    a. The records pertinent to Emeritus Group shall be retained and stored as per the Control of Record Procedure.

    b. Information Labelling and Handling Guidelines and Media Disposal Procedure shall be applicable to records pertinent to Emeritus Group.

    c. The review period and review rights of Emeritus Group institutionalised records shall be defined; and

    d. The backup of records pertinent to Emeritus Group shall adhere to the Back-up Procedure.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Same measures apply to sub (sub-) processors.