**­**

Information Technology

& Security Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Name** | **Designation** | **Date** | **Signature** |
| Initiated by |  | Deputy Governor – Corporate Resources |  |  |
| Endorsed by |  | Governor |  |  |
| Approved by |  | Board of Directors |  |  |

**Amendment History Sheet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No.** | **Revision Date** | **Details of Amendment** | **Originated By** | **Approved by** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
|  |  |  |  |  |

**Distribution List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No.** | **Name** | **Designation** | **Department** |
| 1 |  |  |  |
| 2 |  |  |  |
|  |  |  |  |

**List of Applicable Laws, Regulations and Guidelines**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No.** | **Name** | **Authority** | **Date** |
| 1 |  |  |  |
| 2 |  |  |  |

Table of Contents

[Section A – Overview 4](#_Toc22662790)

[1. Introduction 5](#_Toc22662791)

[2. Scope 5](#_Toc22662792)

[3. Manual Control and Distribution 6](#_Toc22662793)

[Section B – IT Strategy & Governance 7](#_Toc22662794)

[4. IT Strategy 8](#_Toc22662795)

[5. Performance Management 8](#_Toc22662796)

[6. Service Level Management 8](#_Toc22662797)

[7. Enterprise Architecture 9](#_Toc22662798)

[Section C – IT Project Management 10](#_Toc22662799)

[8. Project Management 11](#_Toc22662800)

[9. Release and Deployment Management 12](#_Toc22662801)

[Section D – IT Asset Management 13](#_Toc22662802)

[10. Purchase of Assets 14](#_Toc22662803)

[11. Hardware Asset Management 14](#_Toc22662804)

[12. Software Acquisition and Management 15](#_Toc22662805)

[Section E – IT Development and Change Management 16](#_Toc22662806)

[13. In-House Development and Modifications 17](#_Toc22662807)

[14. Change Management 17](#_Toc22662808)

[Section F – IT Service Management 19](#_Toc22662809)

[15. Incident Management 20](#_Toc22662810)

[16. Request Fulfilment 20](#_Toc22662811)

[17. Problem Management 21](#_Toc22662812)

[18. Service Desk Management 21](#_Toc22662813)

[19. User Access Management 23](#_Toc22662814)

[20. Supplier Management 23](#_Toc22662815)

[21. Backup Management 23](#_Toc22662816)

[22. Data Disposal & Media Destruction 24](#_Toc22662817)

[23. Disaster Recovery Management 25](#_Toc22662818)

[24. IT Awareness, Training and Communication 26](#_Toc22662819)

[Section G – IT Security Management 27](#_Toc22662820)

[25. Information Security Management 28](#_Toc22662821)

[26. Information Security Management Risk Assessment 28](#_Toc22662822)

[27. Third Party Supplier Security 29](#_Toc22662823)

[28. User Accounts and Devices 29](#_Toc22662824)

[29. Acceptable IT Usage 30](#_Toc22662825)

[30. Incident Prevention 32](#_Toc22662826)

[31. Human Resources Security 33](#_Toc22662827)

[32. Employee Responsibility 33](#_Toc22662828)

[33. Termination & End of Employment 34](#_Toc22662829)

[34. Physical and Environmental Security 34](#_Toc22662830)

[35. Access Control 36](#_Toc22662831)

[36. Security Incident Management 38](#_Toc22662832)

[37. Compliance and Review 38](#_Toc22662833)

[Section H – Information Classification 40](#_Toc22662834)

[38. Information Classification 41](#_Toc22662835)

[39. Change of Classification 43](#_Toc22662836)

[40. Recipient 43](#_Toc22662837)

[41. Reporting and sanctions 44](#_Toc22662838)

[Appendices 45](#_Toc22662839)

[Appendix 1: Definitions 46](#_Toc22662840)

[Appendix 2: Abbreviations 47](#_Toc22662841)

[Appendix 3: List of Forms and Templates 48](#_Toc22662842)

[Appendix 4: Information Classification Guidelines 49](#_Toc22662843)

Section A – Overview

1. Introduction
   1. The Real Estate General Authority’s, later on (“REGA” or “Authority”), Information Technology & Security (“IT”) Department is responsible for enabling the Authority with its day-to-day IT operations. Specifically, the IT Department shall be responsible for activities related to the following:
      1. Manage financial planning, budgeting, forecasting and reporting;\*
      2. Manage all IT and technology-related projects within the Authority;
      3. Ensuring smooth operational running of the Authority’s IT systems;
      4. Ensure proper backup procedures for Information Security;
      5. Provide high quality IT services to users in all functions;
      6. Provision of IT security for applications;
      7. Manage all administrative functions;\*
      8. Ensure effective IT security for the organization; and
      9. Manage all procurement activities.\*

\*From a technology enablement perspective

* 1. The Authority’s IT Policy “this Policy” sets out the policies that are to be followed by the Authority, its managers and employees as well as suppliers and contractors, where applicable, while carrying out IT activities.
  2. This Policy is written in compliance with the relevant Laws and Regulations “the Laws”. In case of any discrepancies between this Policy and the Laws, the Laws shall prevail.

1. Scope
   1. This Policy covers the following activities for the Authority:
      1. IT Strategy and Governance;
      2. IT Project Management;
      3. IT Asset Management;
      4. IT Development and Change Management;
      5. IT Service Management
      6. IT Security Management; and
      7. Information Classification.
   2. This Policy shall be read in conjunction with the IT Procedures Manual for further guidance on how to execute these policies.
2. Manual Control and Distribution
   1. The General Manager of the Information Technology & Security Department (“ITGM”) is the custodian of this Policy. The ITGM is expected to ensure that this Policy is a true and accurate representation of the applicable policies and that it is kept up to date at all times.
   2. This Policy shall be made available to the employees in a non-editable version. All employees who are involved in IT-related activities shall have a thorough understanding of this Policy. The Authority's IT procedures shall be executed in accordance with this Policy.
   3. All requests for revisions shall be addressed to the ITGM. This Policy shall be reviewed annually or more frequently if required. Amendments shall be made, if any are required, after approval as per the DoA, and superseded versions of the policies and procedures shall be retained for future reference.
   4. Compliance to this Policy is mandatory and any exceptions shall be pre-approved by the BoD.

Section B – IT Strategy & Governance

1. IT Strategy
   1. The IT Department shall develop an IT Strategic Plan by setting the vision, mission and objectives of the IT Department through the involvement of the Authority’s key stakeholders.
   2. The IT Department shall be responsible for periodically liaising with the Authority’s higher management and relevant stakeholders to ensure alignment of the Authority’s IT and the Authority’s strategy objectives in order to maximise the value delivered by the IT Department.
   3. The IT Department shall be responsible for prioritising strategic projects based on a gap assessment between the Authority’s strategy and organisational requirements as compared with existing IT processes, applications, infrastructure and human capital.
   4. The IT Department shall develop a list of proposed IT projects and preliminary cost estimates as part of the IT Strategic Plan.
2. Performance Management
   1. The ITGM is responsible for establishing a performance mechanism at the IT department to evaluate the department’s operational performance on an annual basis.
   2. The IT Department shall be responsible for establishing the process and tools required to collect data for reporting on performance measures, and shall review the captured data and information to assess the level of services provided and to periodically identify improvement opportunities.
3. Service Level Management
   1. The IT Department may establish service level management activities with other departments within the Authority and other external stakeholders, if any, to ensure that service delivery is reliable, responsive, effective and efficient, and supports the Authority’s requirements to an acceptable level. This involves understanding the IT requirements of the users and working within the constraints of the resources available to agree to a level of service that users can expect consistently.
   2. The IT Department may establish Service Level Agreements (“SLA”) with its users, which would refer to a committed timeframe between the IT Department and its users in order to resolve requests and by taking into consideration the assigned priority levels (as shown in ‎18.5).
   3. The IT Department shall define its SLAs as per the scope of services and as part of the contractual agreement with the relevant Service Provider.
4. Enterprise Architecture
   1. The IT Department shall analyse its Enterprise Architecture on an annual basis to ensure that the current architecture achieves the right balance of efficiency and innovation and is suitable to incorporate the Authority’s strategy and growth plans.
   2. The IT Department shall develop a target Enterprise Architecture, aligned against the baseline architecture. The IT Department shall consider the overall Enterprise Architecture in the set up and review of the IT architecture by documenting gaps between the baseline and target architecture.
   3. The IT Department shall ensure that any changes to the architecture requirements are communicated, documented and analysed to understand the full implications.
   4. The IT Department shall rationalise the gaps between the target and baseline architectures by accounting for both technical and organisational requirements and grouping them into proposed projects and initiatives.

Section C – IT Project Management

1. Project Management
   1. The IT Department shall undertake a structured approach to its project management activities and aim to deliver maximum value to its stakeholders by executing these projects in a timely manner, within the agreed budget, in adherence to their quality requirements and in a risk-managed environment.
   2. Upon receipt of a project request from internal stakeholders, the IT Department shall develop a Business Case in order to assess the prospective project’s feasibility and alignment with the Authority’s strategy and submit for approval as per the DoA in coordination with the Project Management Office (“PMO”).
   3. The IT Department shall upload the project information/requirements on the relevant project management module in coordination with the PMO after obtaining the necessary approvals on the Business Case.
   4. The ITGM shall assign a Project Manager from within the IT department.
   5. The IT Department shall develop a Project Charter, which may include the following:
      1. Project Justifications and Organisational Requirements (including a description);
      2. Establishment of clear and achievable objectives, with the defined delivery approach;
      3. Balancing the competing demands of scope, time, cost, quality and risk; and
      4. Adapting the specifications, plans, and approach the different concerns and exceptions of the various stakeholders.
   6. The IT Department may establish an appropriate Project Steering Committee, in coordination with the PMO, for its projects once the Project Charter has been approved. The Project Steering Committee shall hold ultimate authority and accountability for the effective governance of a project.
   7. The designated Project Manager shall be responsible for the development of a Project Plan and for other parameters such as the following - budget, quality, risk, timelines, execution and ensuring all relevant information is available to the Project Steering Committee.
   8. The Project Manager shall be responsible of and ensure that the project being undertaken is correctly logged and tracked using the EPM system, in coordination with the PMO, in order to ensure that the Authority’s strategic and organisational objectives are aligned.
   9. The Project scope and success criteria shall be established at the beginning of each project and the Project Manager shall track against the success criteria for the duration of the project until final sign-off by relevant approval authorities.
   10. The designated Project Manager shall lead and manage the execution of all project related deliverables. The project management approach may follow industry recognised methodologies/ standards. The projects shall be monitored on regular basis by the IT Department/ Project Steering Committee for the accomplishment of desired results and any possible variances.
   11. The Project Manager shall refer to the Authority’s Procurement & Contracts & Contracts Policy for all project-related Procurement & Contracts activities.
   12. The designated Project Manager shall ensure timely and periodic reporting to relevant stakeholders, which would provide an accurate view of progress made thus far. All communication shall be as per a pre-established communication plan for project milestones reporting.
   13. All project-related deliverables require approval from the relevant approval authorities and all deliverables shall undergo user acceptance testing, if applicable.
   14. The Project Manager shall escalate any exceptions/ deviations relating to the project with the Project Steering Committee/ User for their inputs and resolution.
   15. All project risks shall be documented to include both a description of the risk (categorised as per probability and impact) and documented responses and actions taken to mitigate such risks.
2. Release and Deployment Management
   1. The implementation plan of upcoming releases shall be based on the project plan.
   2. The release plan for all REGA-related technology projects shall be approved by the ITGM.
   3. Releases shall be deployed only after the requisite User Acceptance Testing (UAT) is conducted.

Section D – IT Asset Management

1. Purchase of Assets
   1. All Procurement & Contracts of hardware and software shall be done as per the Authority’s Procurement & Contracts Policy after obtaining the necessary approvals as per the DoA.
   2. Compatibility of hardware components with the Authority’s systems shall be checked prior to purchase.
2. Hardware Asset Management
   1. The IT Department shall maintain an Asset register, which includes comprehensive details about all IT assets. The information may include the following - date of purchase, date of use, cost of the item, specification and useful life. The Asset register shall capture information on owners assigned for all important assets to provide appropriate protection.
   2. The IT Department shall ensure that all information assets are classified and handled on the basis of its value, legal requirement, sensitivity and criticality to the Authority.
   3. All assets shall be covered under an Annual Maintenance Contract (AMC) with the respective vendors to provide support and the IT Department shall evaluate their performance on a regular basis.
   4. The following documentation may be maintained for managing the hardware assets:
      1. System start-up and shut-down procedures;
      2. Back-up of information and equipment maintenance;
      3. Processing and handling of information;
      4. Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
      5. Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
      6. Support contacts in the event of unexpected operational or technical difficulties;
      7. Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;
      8. System restart and recovery procedures for use in the event of system failure; and
      9. Computer room and mail handling management and safety.
3. Software Acquisition and Management
   1. The IT Department shall take into account the following key considerations while procuring Software:
      1. All purchases shall be done as per the Authority’s Procurement & Contracts Policy; and
      2. Any unauthorised or unlicensed software shall not be procured and used by the Authority.
   2. The functionalities that the software requires shall be defined and analysed in coordination with the relevant stakeholders.
   3. Software contracts shall cover requirements detailing expected quality, acceptable performance, and lead time.
   4. Any software acquired by the Authority shall be used in accordance with licensing agreements.
   5. Employees are not allowed to use software which has not been authorised by the IT Department. Any violations shall be reported to the IT Department.
   6. The IT Department shall monitor software license terms and conditions, including those applying to limited use.
   7. Products licensed to run on a specific computer shall not be copied onto another computer or another site without written authorisation from the vendor.

Open Source Software

* 1. Any new open source software usage request shall be reviewed and approved by the IT Department.
  2. The relevant Department may request the usage of an open source software and shall ensure providing a valid justification.
  3. The IT Department shall, prior to approval, ensure that the open source software requested complies with REGA’s current IT ecosystem and if the application requires any additional opening of any firewall ports.
  4. The IT Department shall ensure that only approved open source software should be used. In case of unapproved usage, the IT Department shall report it to the ITGM to take the necessary action.
  5. The IT Department shall maintain an inventory of all software being used, including open source software.
  6. The IT Department shall ensure adherence to REGA’s IT Security Management Policy when it comes to open source software (refer to section G).

Section E – IT Development and Change Management

1. In-House Development and Modifications
   1. The IT Department shall establish a system development methodology for all application systems, in order to ensure that application systems are developed and implemented efficiently, effectively, and in line with the Authority’s requirements.
   2. A separate library setup shall be kept for all in-house developed system’s codes and objects. The IT Department shall maintain fixed documentation for the library’s list structure in the production environment.
   3. The IT Department shall be responsible for keeping documentation and technical information of each in-house system developed, documentation shall take into consideration:
      1. System Flow Diagram (SFD);
      2. Operational Manual for end users, i.e. step by step procedures with screenshots;
      3. Illustration for technical system flow, list of physical files used with their relationship;
      4. Explanation of the Record Status fields, Record Type fields, Flag fields, etc.; and
      5. Details of system’s integrations with other systems, software’s, applications, etc.
   4. The IT Department shall be responsible for modifications occurring over in-house developed and acquired systems and applications.
2. Change Management
   1. The IT Department shall develop change management standards and methodology to ensure that standardised methods and procedures are used for efficient and prompt handling of all IT related changes, in order to minimise the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the Authority.
   2. Some of the key objectives that shall be addressed by the change management are:
      1. To record all requests for changes to configuration items;
      2. To assess and approve all requests for change before going forward to design and build;
      3. To ensure all changes are fully tested before being implemented, where possible; and
      4. To review all changes that has been implemented to assess their success.
   3. Change management procedure shall define the key process activities methods and techniques which may be utilised in order to have an effective and efficient change management process.
   4. Change Request status shall be logged till its closure.
   5. The IT Department shall establish appropriate methods for testing and deploying new or changed services which enables the planning, tracking and checking of progress against requirements at every stage through the service transition.

Section F – IT Service Management

1. Incident Management
   1. Any unplanned interruption of one or more IT services or a reduction in the quality of one or more IT service may be classified as an incident.
   2. All of the Authority’s asset owners, asset custodians, users, as well as third party contractors are responsible for reporting incidents that affect or might affect the security posture of the Authority. This includes any security breaches, events, weaknesses or incidents to the Help Desk as quickly as possible.
   3. Incidents may be categorised in the following types:
      1. Application or Software - e.g. a software bug is preventing a user from using the application
      2. Hardware - e.g. hardware break down may cause system downtime
      3. Technical incidents - e.g. disk space nearing its full capacity must prevent users from saving large amount of data.
   4. The IT Department shall design and implement incident management procedures in order to ensure that all incidents are resolved and service restored in a timely and effective manner.
   5. The Authority shall ensure that all users are trained to identify and report information security incidents. Examples of information security incidents are:
      1. Malware (e.g. virus/ worm/ Trojan);
      2. Social Engineering;
      3. Unauthorised disclosure of sensitive information;
      4. Theft of assets (e.g. laptop, mobile, sensitive documents, etc.);
      5. Suspicious emails (e.g. spam, phishing email);
      6. Misuse of systems by employees or contractors;
      7. System failures due to a suspected malicious act;
      8. Environmental incidents (e.g. fire, water leakage, etc.); and
      9. Violation of information security policies and procedures.
2. Request Fulfilment
   1. Request fulfilment is the process of responding to standard service requests from all the Authority’s internal stakeholders.
   2. A service request may include requesting for information, or advice; requesting change or services such as network folder access, mailbox creation, breakdown incidents, etc.
   3. The following characteristics constitute a service request:
      1. Standard services for which a pre-defined approval and qualification process exists;
      2. Providing information to the Authority’s internal stakeholders about the availability of certain services and the respective procedure for obtaining them;
      3. Procuring the required components of requested standard services; and
      4. Assisting with general information or comments.
3. Problem Management
   1. Problem Management shall be critical in reducing the number of incidents that interrupt the conduct of the Authority’s work.
   2. Historic information of prior complex incidents shall be documented.
   3. The information shall be easily available in order to be referenced by simple and detectable triggers from new Incidents.
   4. Service desk staff providing the first line of support shall be trained to:
      1. Understand the depth of the information available;
      2. How to access, interpret and resolve the first level issues; and
      3. Their role in providing feedback on its relevance and ease of use.
   5. A suitable repository for the information – typically based on an integrated Help Management tool which can capture it at logging or first-analysis stage - may be used.
   6. There shall be a gradual reduction in the number and impact of problems following resolution. The IT Department shall ensure that the number and impact of known problems and errors are reduced.
4. Service Desk Management
   1. The IT Department shall be responsible for restoring the normal service operation as per agreed SLA’s to minimise the adverse impact on the Authority’s operations.
   2. The Service Desk shall be the single point of contact for all requests whether they are incidents, service requests, changes, outage, notifications, cancellations or recovery of equipment, IT Induction, asset reports, IT contracts or any form of IT purchases.

|  |  |
| --- | --- |
| **Service Operation** | **Triggered by** |
| Incident Management | Incident Request |
| Request Fulfilment | Service Request |
| Problem Management | Complex Incident |
| Access Management | Access related requests |

* 1. The IT Helpdesk Specialist shall analyse the nature of Incident or Service request and shall assign the requisite priority levels.
  2. The IT Helpdesk Specialist shall assign a priority to an Incident or Service request to indicate its relative importance in order to ensure the appropriate allocation of resources and, to determine the timeframe within which action is required.
  3. Service Desk priority levels may be set out as below:

|  |  |
| --- | --- |
| **Priority** | **Description** |
| High | Affecting all the Authority’s employees/ critical applications or infrastructure |
| Normal | Degradation in Performance/ Service |
| Low | Affecting individuals due to failure of software or hardware |

* 1. Some requests for service may require the transfer of knowledge or gathering of information, to continue to track such cases, the IT Helpdesk Specialist may record them as self-tasks and set reminders.
  2. The IT staff assigned the Service Request shall aim to complete the tasks associated with the request within the agreed SLA.
  3. A status of "On Hold" shall indicate that the Service Request may be waiting for input from external Vendors or Service Providers, to where the root cause of the case may have been traced.
  4. A status of "Resolved" shall indicate that all tasks have been completed as per the stakeholder’s request.
  5. It is the responsibility of the IT Helpdesk Specialist to ensure that requests are recorded appropriately and all the necessary details are documented.
  6. The IT Department shall produce reports and metrics which indicate the performance of the IT service and support operations.

1. User Access Management
   1. Access Management is the process of granting access rights to authorised Authority personnel while preventing access to non-authorised users.
   2. Access to information shall be limited to authorised persons whose job responsibilities require it or as determined by the data owner.
2. Supplier Management
   1. The IT Department shall develop a detailed scope of work/ services document, which would stipulate applicable SLA’s and performance reporting requirements, with IT service providers/ third party vendors prior to commencement of their respective services.
   2. The IT Department shall periodically review and score performance of third-party service providers against parameters and measures and share with the Procurement & Contracts Department.
3. Backup Management
   1. The IT Department shall put in place procedures to back up all identified data of the Authority and shall store it securely for retrieval when required.
   2. The backup requirements shall define the following, at a minimum:
      1. Backup frequency (i.e. online, daily, weekly, quarterly, yearly);
      2. Backup responsibilities;
      3. Nature of backup (i.e. full back up, incremental backup);
      4. Media cycling requirements and RTO (i.e. the time period within which the information needs to be restored in the event of unavailability of the primary data), RPO, i.e. the point in time prior to an event or incident to which data can be recovered).
   3. The IT Department shall ensure that the backup requirements are formally documented and made available to the system administrators. The system administrators shall maintain complete records of all backups they have made in line with the backup requirements, including date/time, success/failure and media information.
   4. The IT Department shall prepare a formal backup schedule, which shall be followed for creating copies of production program and data files.
   5. The IT Department shall periodically test the backup media for restorability. There may be two levels of restoration checking – for the usability of the media and for the integrity of the data contained therein. A report after each test shall be submitted to IT Director.
   6. The IT Department shall be responsible for developing a restoration plan, which shall include at the minimum:
      1. Rotation plan for testing recoverability – both media and data integrity;
      2. Frequency of testing; and
      3. Procedures to be performed in case of failure of the recoverability testing.
   7. The IT Department shall incorporate its document retention policy into the backup and media cycling plans, to ensure that these do not violate the retention policies. For example, records required to be maintained for a period of 5 years must be appropriately maintained as full backups and tested for recoverability as per the specified frequency.
   8. The IT Department shall ensure that all data to be archived is backed up on at least two separate media, which must be stored in appropriate physical and environmental conditions suitable to long-term archival. Environmental conditions include temperature, humidity, light; packaging and physical access should be appropriately measured and managed, after assessing their safe levels.
   9. The IT Department shall describe and document who are the personnel authorised to access on-site backup area, off-site storage facility and shall prepare a list of their names and functions.
4. Data Disposal & Media Destruction
   1. The IT Department shall ensure that all sensitive information from processing equipment and storage media must be securely removed prior to disposal or re-use.
   2. The IT Department shall ensure that all equipment containing storage devices are checked for removal or overwriting of sensitive data and licensed software prior to their disposal.
   3. Data which is no longer required should be dealt with appropriately and must be undertaken by appropriately trained IT Department personnel and approved as per the DoA.
   4. The following table lists down the appropriate media destruction methods and mechanisms to be used in order to ensure that data is non-retrievable:

|  |  |
| --- | --- |
| **Media Type** | **Destruction Methods** |
| Hard Disk Drives | Data Wiping/Cleaning |
| CDROM/DVD-R | Physical Destruction |
| CD-RW/DVD-RW | Physical Destruction |
| Magnetic Tape | Physical Destruction |
| Flash Disk Drives | Physical Destruction |

* 1. Mobile devices which are returned and issued for re-use within the Authority must have factory settings restored prior to re-issuing.
  2. Computer hardware which is to remain in use within the Authority, but is relocated to a different department, shall undergo a general re-format of the drive.
  3. Tools that attempt to retrieve data from media which has undergone a data removal process shall be used in order to verify that complete data removal has taken place. If any files or fragments of files are evident, then data disposal has been unsuccessful.
  4. Logs will be maintained with the IT Department of any hardware provided to the IT Department for data disposal together with verification results in order to ensure that all data requiring disposal is correctly organised and properly audited.
  5. The IT Asset Registry shall be used in order to track device serial numbers which are disposed of.

1. Disaster Recovery Management
   1. A Disaster may be defined as a severe or serious incident that cannot be managed within the scope of the IT Department’s normal working operations.
   2. The IT Department shall prepare a Disaster Recovery plan which includes a classification of IT systems and their corresponding recovery objectives based on criticality and the roles and responsibilities of the Authority’s personnel.
   3. The Disaster Recovery Plan(s) (DRP) shall be reviewed for completeness by the IT Department through considering the below:
      1. Possible alternate processing sites;
      2. Alternate sites tested at least annually;
      3. Agreement exist for the use of the alternate sites;
      4. Availability of peripheral equipment;
      5. Defining critical systems to be processed;
      6. Ability to process without key personnel; and
      7. Ability to adapt plan to lesser disasters.
   4. The Authority shall have a Disaster Management Team in place to manage and oversee all recovery operations in event of a disaster.
   5. The Authority shall have a Disaster Response Team in place to execute all the necessary recovery operations in event of a disaster.
   6. The IT Department shall keep an updated list of the Authority employees and third party personnel that shall be contacted in the event of an emergency.
   7. All relevant Authority employees shall undergo training with regard to Disaster Recovery to understand their respective roles and responsibilities.
2. IT Awareness, Training and Communication
   1. The IT Department shall ensure that all Authority staff are equipped with relevant Information Technology related knowledge and skills.
   2. The IT Department shall train all its employees, contracted staff, users and customers to recognise and respond to security incidents. Training shall also be imparted in security procedures and the correct use of information processing facilities to minimise security risks prior to resuming their responsibilities in the Authority.
   3. The IT Department shall provide its Information Security policies to its own staff as well as staff working with any contractors and acknowledge in writing that they understood their responsibilities as stated in the policies.
   4. The IT Department shall share communications with regard to updates on the security policies and processes by various means such as e-mail, intranet and during corporate events and meetings.
   5. The IT Department may coordinate with the Communication and HC Departments to brainstorm innovative methods regarding IT awareness (e.g. content creation, animated videos, etc.)

Section G – IT Security Management

1. Information Security Management
   1. The Information Security Objectives shall provide a framework for defining, implementing, reviewing and updating objectives periodically, in order to ensure the provision of information of security to all the information assets within the Authority’s scope. The Information security objectives defined for the Authority are as follows:
      1. To ensure that information-related operations continue to be carried out based on the Authority’s requirements and the relevant industry cyber security standards.
      2. To protect the Authority’s information to ensure confidentiality and integrity of information and availability of information to authorised individuals;
      3. Successful management of the Authority’s information and information assets.
      4. To proactively manage information security risks;
      5. To enhance information security awareness among the Authority’s employees and vendors;
      6. To ensure the security breaches and information security incidents are managed effectively; and
      7. To establish information security objectives, aligned with continuous improvement best practices. In order to achieve this, specific information security objectives shall be:

* Defined annually, to ensure adequate management approval and budgeting;
* Based on the Authority’s requirements, results from Risk Assessment and management reviews;
* Documented in a plan describing how and when they will be achieved, and;
* Reviewed on a quarterly basis to ensure that they remain valid and implementation is being achieved. Deviations from the plan shall be documented, and if applicable, a corrective plan designed and approved by management.
  1. The IT Department shall ensure that adequate information security skills and expertise are available to the Authority in order to provide information security support and advice.

1. Information Security Management Risk Assessment
   1. The Information Security Management Risk assessment process shall be aligned with the overall risk management methodology and activities in the Authority.
   2. The IT Department shall ensure that the design, implementation and adherence to the Information Security policies are periodically assessed.
   3. The IT Department shall establish and maintain mechanisms to guide the day-to-day activities of the IT custodians to carry out tasks associated with managing and adhering to Information Security requirements across the Authority.
2. Third Party Supplier Security
   1. The IT Department may enter any relationship with an outside Vendor/Expert on an appropriate contract and Service Level Agreement relating to the outsourced service.
   2. The outsourcing contract at a minimum must address the following:
      1. Security responsibilities of all parties involved in the outsourcing, including subcontractors;
      2. Maintenance and testing of the confidentiality and integrity of the Authority’s assets;
      3. Physical and logical controls to limit access to the organisation’s sensitive information;
      4. Availability of services in the event of a disaster;
      5. Physical security requirements for the outsourced equipment and infrastructure;
      6. Legal requirements and the right of audit including third party audits;
      7. Target level and unacceptable levels of each service outsourced;
      8. Intellectual property rights and protection of any collaborative work;
      9. Right to monitor and revoke user activity, and;
      10. Reporting structure and clear reporting formats including reporting, notification and investigation relating to security incidents and breaches.
   3. The IT Department shall identify the risks associated with accessing the Authority’s information and information processing facilities by external parties.
   4. Access to information assets and information processing facilities by all Outsourced Service Providers (OSP) and Third Party staff must be according to the security policy of the IT Department. Access should not be provided until the appropriate controls have been implemented and a Contract has been signed.
3. User Accounts and Devices
   1. The IT Department shall ensure that all internal user accounts have the following password requirements, as a minimum:
      1. Require a unique password, comprised of a minimum of eight alpha-numeric characters that shall be changed at first login;
      2. Passwords shall be changed at least once every 90 days or at a frequency that meets local legal requirements;
      3. Password reuse/ duplication within the 32 previous passwords shall be prevented either by technical measures or by corresponding policies;
      4. Passwords shall be stored using a one-way encryption mechanism;
      5. Applications that allow interactive password changes shall force users to create complex passwords if possible; and
      6. Where supported by the technology in use, internal user accounts shall be configured to lock out after a set number of failed login attempts (15 times).
   2. The IT Department shall ensure that external user accounts which access internet facing applications shall meet the same control requirement as internal user accounts but may extend the password change frequency to 180 days if the application includes mechanisms to enforce both complex password construction requirements and a lock out mechanism that is triggered based on failed login attempts.
   3. The IT Department shall ensure that all workstations, laptops, desktops and other Authority provided devices shall be secured with a password-protected screen saver with an automatic log-off activation feature when left idle for a period of time (15 Minutes). Users shall ensure they manually log-off from any device when the device is not in use.
   4. The IT Department shall ensure that all devices (laptops, desktops, external devices) used by employees and connected to any of Authority’s networks are continuously scanned for viruses and other malware by an approved virus/malware scanning software(s).
   5. The IT Department shall ensure that up-to-date anti-virus software is installed and running on laptops and desktops.
   6. The IT Department shall generate periodic reports to ensure that all devices comply with these policies. These reports may be shared by the IT Department with other Departments or Stakeholders only after permission from the Head of Department.
4. Acceptable IT Usage
   1. All users of the Authority’s IT equipment shall be responsible for exercising good judgement and fair use regarding personal use of IT. The Authority has the right to audit the usage of IT equipment, networks and systems to ensure compliance with the Information Security policy.
   2. Any loss/damage of the Authority owned mobile devices is the responsibility of the designated user and the Authority has the right to recover all associated costs from the employee, if the employee was found to have been negligent.
   3. User departments shall be responsible for the classification of information stored on any of the Authority related internet/intranet/extranet-related and file systems as per the Authority’s Information Classification requirements (refer to Section H).
   4. Users shall take all necessary steps to prevent unauthorised access to classified information. All the data shall be stored only on the IT authorised file servers/disks.
   5. Users shall keep passwords secured and undisclosed. Users shall not share or use shared accounts. Users are responsible for the security of their passwords and users accounts.
   6. Private use of the Authority’s e-mail addresses to external news groups, forums or social media is strictly prohibited, unless required by the Authority’s duties.
   7. Access to the Authority’s emails/ data on personal devices shall be prohibited unless approved by IT Department.
   8. Users shall immediately report any desktop or laptop damages to the IT Department. If any damage is deemed to be caused by the employee, the Authority has the right to recover all costs from the employee if the employee is proven responsible or to have acted negligibly.
   9. Users shall use caution when opening e-mail attachments received from unknown and untrusted senders and sources as such may contain viruses, e-mail bombs, or Trojan horses that can cause major security impact.
   10. Users shall ensure that executable file attachments from unknown and untrusted sources shall never be opened. Users shall seek advice from the IT service desk when receiving suspicious emails.
   11. Users shall ensure that classified data is stored in the appropriate placeholders on the Authority’s network and not retained locally on desktops or laptops.
   12. Users shall ensure that laptop and mobile devices use is restricted to official purpose only. Users of laptops shall comply with the Information Security Policy to ensure confidentiality, integrity and availability of the information stored on the laptop.
   13. Laptop users shall take caution against security threats from the external connections while using the laptop outside the Authority’s premises.
   14. Users shall not leave mobile devices (e.g. laptops, etc.) in unprotected places such as cars, public transport vehicles, suitcases in the baggage hold of an aircraft or any other public places unattended.
   15. Users shall not open classified documents in public places (for example: Company registrations details, etc.) unless required.
   16. Users are advised not to transfer Authority owned or related data out of the Authority’s network and premises without prior written approval from the relevant Head of Department.
   17. Users who have installed third party software shall respect all license agreements and/or copyright laws. It is illegal to have or use copies of software protected by copyright laws and/or license agreements unless the owner of the copyright or license holder specifically gives permission.
   18. Usage and connection of non-Authority provided mobile and other personal devices to the Authority network shall be authorised and shall comply with IT security standards and processes.
   19. Users or asset owners shall delete spam, chain and other junk e-mails without forwarding. Any unrecognised email shall be reported to the IT service desk immediately.
   20. Examples of unacceptable use includes the following:
       1. Formatting of hard disks of workstations, loading or unloading of software, modifications to settings of software installed on Authority owned equipment;
       2. Not bringing timely attention to the IT Department regarding incidents, errors and malfunctioning of equipment and systems;
       3. Violation of personal rights or Authority copyrighted trade secrets, or other intellectual property;
       4. Installation or distribution of "pirated" software products that are not appropriately licensed for use by the Authority;
       5. Introduction of malicious programs into the Authority’s information process environment;
       6. Logging into a server, system or service that the employee is not authorised to access;
       7. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a system’s or a user's terminal session locally or via the internet/intranet/extranet;
       8. Providing information about the Authority’s employees email addresses to third parties without proper authorisation to do so; or
       9. Sending unsolicited e-mails, including sending of "junk mail" and other advertising material to individuals who did not specifically request such material.
5. Incident Prevention
   1. The following actions by the Authority employees can help prevent information security incidents:
      1. Employees and third party personnel shall display proper badge when in any Authority facility;
      2. Employees shall be aware of their physical surroundings, including weaknesses in physical security and the presence of any unauthorised visitor;
      3. Employees and third party personnel shall use only approved computer hardware and software with the latest patches installed;
      4. Employees and third party personnel shall not download, install, or run a program unless they know it to be authorised by a person or company that they trust;
      5. Employees and third party personnel shall be aware of unexpected attachments when using e-mails; and
      6. Employees shall be aware of social engineering attempts to solicit restricted information, such as account numbers and passwords.
6. Human Resources Security
   1. The IT Department shall ensure that all Information security responsibilities and duties shall remain valid after termination or change of employment of the employee.
   2. The IT Department shall ensure that all employees and third-party personnel sign confidentiality agreement (e.g. Non-Disclosure Agreement) in addition to the employee’s contract.
   3. External staff working on systems used to process the Authority’s information must abide by the Information Security policies and may be asked to sign additional confidentiality Agreements.
7. Employee Responsibility
   1. The IT Department shall ensure that employees, contractors and third party users understand their responsibilities and are suitable for their roles they are considered for, so as to reduce the risk of theft, fraud or misuse of computing facilities and to apply security in accordance with established policies and procedures of the Authority.
   2. Security roles and responsibilities of employees, contractors and third party users shall include the requirement to:
      1. Implement and act in accordance with the Authority’s Information Security policies;
      2. Protect assets from unauthorised access, disclosure, modification, destruction or interference;
      3. Execute particular security processes or activities;
      4. Ensure responsibility is assigned to the individual for actions taken; and
      5. Report security events or potential events or other security risks to the organisation.
   3. All employees and contracted staff must be made aware of what constitutes a security incident and the different types of incidents:
      1. Security breach or violation which means external or internal act that bypasses security policies, practices or procedures;
      2. Threats which are actions or potential occurrence of events to breach the security of the system by exploiting its known or unknown vulnerabilities;
      3. Malfunction which means the failure of the security controls of the system to function properly; or
      4. Weakness which is the flaw in the system that could increase the risk of failure.
   4. Employees have a responsibility to ensure the security and integrity of information and systems and shall comply with the Authority’s Information Security policies and standards. Individuals shall be held accountable for their usage of the Authority’s information processing systems.
   5. Non-compliance or violation of the Information Security Policies and standards may result in action that may include, but not be limited to, the following:
      1. Termination of employment;
      2. Other disciplinary action; and/or
      3. Civil and/or criminal prosecution.
8. Termination & End of Employment
   1. The IT Department shall revoke physical access and network access to all information systems by the last working day of the employee.
   2. The IT Department shall issue a No Objection Clearance (“NOC”) to the employee only after all the Authority’s information assets issued to the Employee are returned before the last working day.
   3. The IT Department shall ensure that any job change (inter-department) will trigger a review of access privileges to systems and assets. These privileges shall be modified according to the new role.
9. Physical and Environmental Security

Working in Secure Areas

* 1. The IT Department shall ensure the physical security and availability of its information systems by protecting them from environmental threats and unauthorised physical access.
  2. The IT Department shall satisfy itself that the requirements of this policy can be met in all areas where Authority information assets are located or planned to be located, before locating any information assets at any location.
  3. While locating information processing equipment, the IT Department must consider the following, at a minimum, to ensure adequate security:
     1. Minimise unnecessary access into work areas;
     2. Segregate the IT equipment used by the Authority employees and those used by third parties;
     3. Minimise risk of potential threats to the equipment such as fire, theft, dust, smoke and water;
     4. Minimise the impact of a disaster within close proximity of the Authority’s premises; and
     5. The backup media storage must be kept at a safe distance of approximately 5 KM from the main site to ensure recoverability in case of disaster at the main site.
  4. The IT Department shall ensure Information processing equipment is kept in suitably designed secure areas based on their risk profile and vulnerability to security threats.
  5. The IT Department shall ensure that all equipment such as servers, network devices, security devices, storage systems, mobile computing devices etc. are put through maintenance process once a year by vendor or by using trained internal personnel. The maintenance Contracts for all the devices shall be kept updated by reviewing them every year.
  6. The IT Department shall ensure that all information assets are insured against personal damages, external damages and threats, to minimise financial losses to the Authority.
  7. The IT Department shall ensure that access is granted only to authorised personnel for secure areas of IT operations. This shall be approved as per the DoA.
  8. The IT Department shall, in coordination with the Facilities Department, have protective measures such as locked, secure doors and perimeter security systems such as access control systems and cameras.
  9. The IT Department shall ensure that access to the information processing facilities by vendors or visitors shall be granted only after authorisation of the ITGM.
  10. The IT Department shall ensure that wherever physical access to sensitive or critical systems is required, the visitor shall be escorted by an IT Employee after acquiring appropriate authorisations.
  11. The IT Department shall ensure that the visitor’s and the escorting personnel’s identities, their date and time of entry and departure are logged for future traceability.
  12. The IT Department shall ensure that all unmanned secure IT areas are physically locked and periodically checked.
  13. The IT Department shall periodically review and update users’ physical access rights to areas where sensitive or critical systems are hosted.
  14. The IT Department shall ensure that environmental conditions that can adversely affect the performance of information systems inside the data centre is monitored and maintained using adequate air and humidity controlling equipment.
  15. The IT Department, in coordination with the Facilities Department, shall ensure an uninterrupted power supply or a planned shutdown of its information systems in the event of a power failure through UPS or back-up generators.
  16. The IT Department shall ensure that smoking, eating and drinking is prohibited inside the server rooms.
  17. The IT Department shall ensure that all hazardous and combustible materials are stored at a safe distance from data centre and information processing facilities.
  18. The IT Department shall coordinate with the Facilities Department in order to ensure that manufacturer’s instructions for protecting equipment are observed at all time.

Clear Desk and Clear Screen

* 1. The IT Department shall promote clear screen policy for its information processing equipment and an Authority-wide clear desk policy to reduce the risk of unauthorised access or loss of confidential information.

1. Access Control
   1. The IT Department shall design and implement an access management framework and supporting procedures and tools, which at a minimum include:
      1. Access to the Authority’s information and system resources shall be given on a need-to-know basis and specific to each employee’s role and responsibility.
      2. All access shall be authorised by the team responsible for the relevant system, application or data.
      3. Employees with the need to have privileged access shall use a separate, non-privileged account for performing normal activities until compensating controls are in place to monitor the privileged activities.
      4. All user accounts shall be individual identifiable and require a unique ID. New user accounts and passwords shall be issued to employees in a secure manner.
      5. All service and user accounts shall be password protected that meets the formal password policy requirements.
      6. System and service account passwords shall be managed and stored in a secure manner.
   2. The IT Department shall periodically review the appropriateness of users’ access rights (minimum annually) for the Data, system and applications.
   3. The IT Department shall design and implement Segregation of Duties standards and rules including supporting procedures. The scope shall include: organisation-wide functions, roles as well as within each critical systems and application.
   4. The IT Department shall ensure that access to system privileged utilities and tools with the capability to override and change existing security controls and configurations is provided only to a limited number of authorised individuals.
   5. The IT Department shall monitor service accounts and review access thereto on a regular basis.
   6. Applications that cannot be secured using built-in system security shall be documented, and the IT Department shall ensure that the following controls at a minimum are programmed into the application:
      1. Edits on data fields;
      2. Secondary passwords;
      3. Exception reports; and
      4. Audit trails.
   7. The IT Department shall determine whether procedures have been developed for reporting and following-up on security violations.
   8. The IT Department shall install printers that support enabling of authentication to prevent sensitive printed information being circulated in an unauthorised manner.

Event Logging and Monitoring

* 1. The IT Department shall design and implement event logging and monitoring procedures for monitoring activities on systems, applications and data. These procedures shall be based on risk assessments, but shall, as a minimum, include:
     1. Authority’s network, systems and applications shall be proactively monitored to detect suspicious and unauthorised events.
     2. Privileged access activities on systems, applications and data shall be logged and retained for a minimum of 1 year.
     3. Critical application and system logs shall be reviewed on a periodic basis. Appropriate protection and controls shall be implemented on all logs.
  2. Upon significant access violations, the IT Department shall ensure that there are inquiry letters written by the Information Security Specialist to the Users’ Head of Departments. Responses received shall be reviewed for explanations of violations.
  3. The IT Department shall determine if a procedure is in place to provide a report for each user, identifying the respective Department’s responsible transactions and the authorised users for those transactions. These reports shall be provided at a minimum every 6 months.

1. Security Incident Management
   1. The IT Department shall design and implement security incident management procedures and supporting tools. All employees, third party personnel and other relevant stakeholders shall receive training of these procedures and be made aware of what constitutes a security incident and how to report it.
   2. Reportable incidents include, but are not limited to, the following:
      1. Physical loss, theft, or unauthorised destruction of the Authority’s information resources, such as, missing or damaged hardware, software, or electronic media;
      2. Unauthorised disclosure, modification, misuse, or inappropriate disposal of the Authority’s information;
      3. Internal or external unauthorised access attempts to access information or the facility where it resides;
      4. Unauthorised activity or transmissions using the Authority’s information resources;
      5. Information resources with virus protection software that is not patched to the current level or is disabled;
      6. Sudden unavailability of files or data normally accessible;
      7. Unexpected processes, such as e-mail transmissions that start without user input;
      8. Systems displaying strange messages or mislabel files and directories;
      9. Detection of unauthorised personnel in controlled information security areas;
      10. Security violation, suspicious actions, or suspicion or occurrence of embezzlement or other fraudulent activities; and
      11. Revenue loss involving an information system.
2. Compliance and Review
   1. The IT Department shall comply with any statutory, regulatory or contractual obligations and the requirements as specified in its information security policies. Periodic compliance audits may be carried out to detect any policy breaches.
   2. The use of commercial applications and operating systems must be in accordance with the related license agreement. Controls shall be enforced to prevent violation of the licensing requirements.
   3. The IT Department must ensure that:
      1. Software copyright compliance policy defining the legal usage of the software is published;
      2. Standard procedures are followed for acquisition of software products;
      3. Awareness is developed among the staff for using only legal copies of software and disciplinary action is taken against users breaching these policies; and
      4. Regular checks are carried out to ensure that only authorised software and licensed products are installed.
   4. The IT Department shall control and maintain software licenses to ensure protection against default or contractual and/or other limitations and liabilities.
   5. The owners, custodians and administrators of the information systems at the Authority shall perform self-assessments to ensure technical compliance. This self-assessment must be performed twice in a year.
   6. The IT Department shall perform a periodic internal and external vulnerability assessment to ensure compliance with organisational security policies. This shall be performed at least yearly.

Section H – Information Classification

1. Information Classification
   1. The classification of information is intended to aid in defining the principles and rules regarding the protection of information within the Authority, whether the concerned information is the property of the Authority or not.
   2. The Information policy applies to all information assets (see Appendix 4 – for definitions of information assets) that is owned by the Authority as well as all non-proprietary information that includes, but is not limited to, customer information.
   3. On matters of information security, users shall refer to the IT Security Management section (refer to Section G – IT Security Management) and shall get in touch with the Information Security Specialist or alternatively the IT Help Desk for further clarifications.
   4. The rationale in classifying information into groupings and classes is so that the Authority will be able to correctly and appropriately allocate resources for the protection of data assets, as well as determining the associated risks involved, such as but not limited to:
      1. Unauthorised disclosure
         * Confidential data will not be accessed by any unauthorised personnel whether internal or external to the Authority.
         * Customer personal data will not be disclosed to unauthorised or unintended recipients whether internal or external to the Authority.
      2. Unauthorised modification to data; and
         * Data integrity is especially important in handling customer information.
      3. Non-availability of data.
         * The risk that data cannot be accessed when required due to systems that either store or carry the data are no longer functioning. An example of this is a denial of service attack.

Public Information

* 1. The Authority considers information public if it has been expressly authorised for public disclosure. Public information shall be disseminated via channels authorised and set by the Management. This may include press release, magazine articles, the Internet (public REGA home pages or mail shots). There are no adverse security concerns if information classified as public is intercepted by external parties. Examples of public information include:
     1. Released marketing material;
     2. Press releases;
     3. Fee pricing information; and
     4. Manuals/Guidelines.

Internal Information

* 1. The Authority considers as internal (“REGA Internal”), any information that has not been expressly authorised as public. This is defined as any data that derives its economic value from not being publicly disclosed. It includes:
     1. Information which the Authority is under legal or contractual obligation to protect; and
     2. Information, whose value, in monetary terms, would diminish if it were to be publicly disclosed; and
  2. Information under this category can be copied and distributed within the Authority to authorised users.
  3. The Authority’s internal classified documents may be disclosed to external entities under a non-disclosure agreement or under explicit authorization by the Information owner/management. Examples include:
     1. Internal phone directories;
     2. Staff HR information;
     3. Organizational structure;
     4. Internal communication to all staff members; and
     5. Internal mailing list.

Confidential Information

* 1. Under this classification, (“REGA Confidential”) information is not to be publicly disclosed, regardless of its economic value. Public disclosure of information that is classified as REGA Confidential will have adverse effects on the Authority and could possibly have significant civil, economic, or criminal liability. Staff members who receive REGA Confidential information shall not reveal the contents to another individual unless that person has a valid need to know the information and has been explicitly authorised by the management to receive such information. Examples of REGA Confidential data include, but are not restricted to:
     1. Company strategic plans;
     2. Server passwords;
     3. Cryptographic keys;
     4. E-commerce transactions;
     5. Organizational charts;
     6. Policy statements, etc.;
     7. Market research studies;
     8. Information on the pricing of fees and services;
     9. Investment plans;
     10. Financial forecasts;
     11. Collective bargaining agreements;
     12. Legal files (contracts, disputes, etc.);
     13. Information on public procurement and civil contracts;
     14. Network diagrams;
     15. Technical equipment set up;
     16. Development and research projects;
     17. The Authority’s various databases; and
     18. Software and related documentation.

Default Classification

* 1. REGA Internal information shall be the default classification. Any information that has not yet been given a classification or any document that has not been labelled with a classification shall be considered automatically classified as REGA Internal.

1. Change of Classification
   1. It should be noted that the category of information’s classification could change during the course of its existence. A document can, for example, during its development process, be considered as REGA Confidential and later on enter the category REGA Internal when it is approved by the appropriate internal authorities and communicated to all staff. In the same spirit, information can lose its confidentiality label when it is, for example, made public or when it loses its competitive value.
2. Recipient
   1. The recipient of confidential information must ensure that the proper procedure as highlighted in the guideline in Appendix 4 is observed in order to prevent non-authorised disclosure.
3. Reporting and sanctions
   1. Any non-authorised disclosure of confidential information must be immediately reported to your line manager or to the IT Department. Any violation of this policy may entail a sanction leading to disciplinary action as prescribed in the HC Policy or as deemed necessary by the management.
   2. The need to protect information is a basic one. However, it may not be misused by withholding information from other staff members under the pretext of confidentiality. Information must be used in the most efficient and flexible way possible, whilst observing the rules of confidentiality.

Appendices

Appendix 1: Definitions

“Access” is anyone who has the right, opportunity, means of finding, using or retrieving information.

‘‘Agreement” means an agreement or understanding between the Authority and a third party that obliges one or both parties to enter into obligations, including without prejudice to generality, non-binding undertakings such as memoranda of understanding, amendment or modifications of existing contracts or similar documents.

“Asset” refers to the Authority-owned information, systems or hardware that is used in its activities.

“Contract” means an agreement or understanding between the Authority and a third party that obliges one or both parties to enter into legally binding obligations.

“Department” means an individual department within the Authority.

“Enterprise Architecture” means a conceptual document which outlines the baseline and target structure to achieve the current and future objectives of the Authority with the goal of having a unified IT structure.

“Laws and Regulations” means all relevant legislation, laws, regulations and standards.

“Service Desk” is intended to provide a single point of contact ("SPOC") to meet the communication needs to all employees (IT users).

“Service Level Agreement” is a written agreement between a service provider and the customer that documents the agreed service levels for a service, defining the key service targets and the responsibilities of both parties.

**“Third party”** is an organisation or person that is not a part of the Authority.

Appendix 2: Abbreviations

| Terms | Definition |
| --- | --- |
| **AMC** | Annual Maintenance Contract |
| **DoA** | Delegation of Authority |
| **DRP** | Disaster Recovery Plan |
| **EPM** | Enterprise Performance Management |
| **ITGM** | General Manager – Information Technology & Security |
| **IT** | Information Technology |
| **NDA** | Non-disclosure Agreement |
| **NOC** | No Objection Clearance |
| **OSP** | Outsourced Service Provider |
| **REGA** | Real Estate General Authority |
| **RTO** | Recovery Time Objective |
| **RPO** | Recovery Point Objective |
| **SFD** | System Flow Diagram |
| **SLA** | Service Level Agreement |
| **UAT** | User Acceptance Testing |

Appendix 3: List of Forms and Templates

| Sr. | Forms and Templates |
| --- | --- |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |
| 11 |  |
| 12 |  |
| 13 |  |
| 14 |  |
| 15 |  |
| 16 |  |
| 17 |  |
| 18 |  |
| 19 |  |
| 20 |  |

Appendix 4: Information Classification Guidelines

Information Owner

The owner of information is the person or entity authorised by the Authority to process that information in accordance with policy (creation, modification, addition, and deletion of information or parts thereof). His/her name or its reference must be clearly mentioned on every supporting document.

Information Custodians

Information custodians are persons or entities that have been authorised by the Authority to store and transfer information assets in accordance with policy. Custodians are NOT authorised to modify, add to, or delete in any way information they have custody to.

Information Assets

All company information, in whatever form (paper documents, computer files, information communicated verbally, registration, etc.) shall be the exclusive property of the Authority in the same way as physical assets such as company vehicles, furniture, equipment, etc. For this reason, employees have no proprietary rights whatsoever with regard to such information.

Handling of "Public" information

As there are no restrictions on public information, it will not be considered further.

Handling of "REGA Internal" information

Distribution, copying and returning

1. Information of this category may be distributed freely within the Authority. This information may be disclosed outside the Authority only if the owner authorizes this. If the owner is not clearly defined, contact your immediate superior for approval. Information of this kind is not subject to restrictions as far as duplication is concerned. Any “REGA Internal” information must always be returned to the Authority by anyone leaving the company.

Mailing and transmission

1. Use envelopes for internal mail. No other particular protective measures have to be taken when transmitting "REGA Internal"-information internally. When transmitting externally using mail, use opaque, non-reusable, closed and correctly addressed envelopes.
2. Double-check the address or the list of addressees before transmitting the information by e-mail.
3. For a fax, always use a cover sheet and double check the recipient’s details. Make sure the information is sent to the correct number and if necessary warn the recipient before you transmit the information.
4. Before disclosing information by phone, make sure your correspondent is authorised to know about it. When in doubt, consult your immediate superior.
5. Speech; be aware of your surroundings - do not discuss this kind of information in the presence of persons from outside the company or in public places (e.g. in a restaurant, on the public transport, etc.)

Filing and storing

*On-site:*

1. Observe the "Clean Desk Policy" and systematically put information in a locked item of furniture at the end of the working day. Remove used flipchart sheets and wipe off whiteboards.

*In- and out-trays:*

1. Make sure all in and out-trays are emptied daily, as well as the in and out-trays of colleagues who are absent or on leave.

*Computer files:*

1. Preferably store information on a network server, a diskette or any other removable magnetic support.
2. Avoid using your local hard disk especially if shared between multiple users.
3. Ensure proper rights are assigned to such files to prevent information theft or leakage.

*Off-sites:*

1. Never leave internal information unattended when you are off the company’s premises (in a car, hotel room, meeting room, seminar, etc.).

Disposal and destruction

1. Always use an office waste or recycling bin to dispose of documents with this indication. Make sure all temporary or backup files are also properly disposed of.

Handling "REGA, Confidential" information

Distribution, copying and returning

1. "REGA Confidential" information is only to be distributed within the Authority on a need-to-know basis. Make sure the recipient is authorised to receive it. When in doubt, consult your immediate superior.
2. If you do not have any need to know about this information, do not attempt to gain access to it.
3. "REGA Confidential" information can only be disclosed to outsiders if prior approval by the concerned Department’s General Manager has been given and if the recipient has signed a non-disclosure agreement or is bound by professional secrecy. Contact the Legal Department for further information.
4. The only exception to this rule can be made for standard contracts or agreements previously submitted for approval to the Legal Department (e.g. a consultancy contract, requests for a study, a benchmarking contract, etc.)
5. Personal information and any customer-related data can only be disclosed outside the Authority, in accordance with certain principles defined by law. Should you require further information, contact the Legal Department.
6. Reproduction of "REGA Confidential" information must be limited to the strict minimum of copies required. All copies must be treated with the same care as the originals.
7. The owner may judge that the information is sufficiently sensitive for a total ban on reproduction. In this case, the information must not only bear the confidentiality label on each page, but also the message "No copies allowed".
8. Another way to make sure this prohibition is observed is the transmission of a registered copy. The name of the recipient should be clearly mentioned on each page, which allows for increased responsibility of the recipient and, if necessary, easier tracing of the person who made the unauthorised copies.
9. "REGA Confidential" information must not only be returned by personnel leaving the company, but also by personnel no longer needing to know it, for example, in the context of a change of activities.

Mailing and transmission

1. "REGA Confidential" information must be placed in a closed, opaque, non-reusable and correctly addressed envelope. If you consider information particularly sensitive or strictly private and you do not want the mail to be opened by a third party (assistant, secretary, etc.), the envelope must not only bear the confidentiality indication, but also the message: "To be opened by the addressee only".
2. The information must, preferably, be transmitted personally. If this proves impossible, the transmittal mode must be identified depending on whether the information must be transmitted internally or externally.
3. If the mail is destined for internal distribution, put the envelope in a second standard envelope used for internal mail. Indicate the complete and accurate addressee’s details. No confidentiality label must be put on the second envelope in order to avoid indiscretion.
4. If the mail is destined for external distribution, put it in a second, closed, opaque, non-reusable and correctly addressed envelope. Do not affix any confidentiality label to the second envelope and send the whole thing by registered mail with possible confirmation of receipt.
5. When sending "REGA Confidential" information, whether internally or externally, to a group of persons, add a list of recipients. This will enable you to check mailing shots better and will have as an advantage that the recipients know with whom they can discuss the information.
6. When sending "REGA Confidential" information by e-mail, double check that you are using the correct mail address. When using predefined address lists, double check that all persons included on these lists are authorised to receive the information. Do request for a proof of submission, and delivery. Never send confidential, unencrypted information over public networks, such as the Internet.

When faxing "REGA Confidential" information to someone:

1. Call your contact by phone to ensure that someone authorised to receive the information is ready to receive it.
2. Double check the recipient’s details before sending the information.
3. Always use a cover sheet.
4. Call to be sure that the documents have been received correctly.

Before disclosing "REGA Confidential" information by phone:

1. Double check the person is authorised to receive the information.
2. Tell your correspondent beforehand that the information is strictly confidential.

Do not discuss "REGA Confidential" information:

1. In the presence of persons from outside the company.
2. In public places (in a restaurant, on the public transport, during seminars, etc.)
3. In the presence of personnel of the Authority not authorised to know.

Filing and storing On-site

1. In addition to the "Clean Desk Policy", "REGA Confidential" information must always be stored in locked items of furniture to which a limited number of authorised people have access.
2. Remove used flipchart sheets and wipe whiteboards.
3. Offices and meeting rooms with confidential information must be locked when you leave the room, even for a brief moment. The most sensitive information must be stored in fireproof safes to which a limited number of authorised people have access. An inventory of documents contained in these safes must be made and kept up to date. Make sure that your in- and out-trays are emptied daily, as well as the in- and out-trays of colleagues who are absent or on leave.
4. Store files containing "REGA Confidential" information only on protected systems and/or network drives. In case of the information being stored on a diskette or any other removable magnetic media ensure that all necessary measures are taken for the physical protection of the media. Removable media must be treated with the same care as paper supports and hence be stored in a locked desk or cabinet or in a fireproof safe. Never store information on your local hard disk that are shared with other users. Even in case where users have discrete access to the computer, special care must be taken to ensure that rights assigned on the information do not compromise the security of data. It is recommended to encrypt “REGA Confidential” data during long-term storage.

*Off-site:*

1. Be sure never to leave "REGA Confidential" information unattended when you are off the Authority premises (in a car, hotel room, meeting room, seminar, etc.).

Disposal and destruction

1. All "REGA Confidential" must be disposed of in a secure way. Paper must be shredded. Hard disk drives must erased using software specifically designed to erase data by 3 levels of write function to the drive. Magnetic Tapes should also be erased or overwritten with data as recommended by Security best practices to ensure destruction of original data.

Releases to the media

Any information to be disclosed to the media, even if it does not belong to one of the two categories, may only be communicated after prior agreement of the "Communication Department" as per the Authority’s DoA.