INFORMATION SECURITY POLICY

POL 41/2020

Commencement Date	1 April 2020
Review Date	31 March 2021

POLICY STATEMENT

1 Introduction

The confidentiality, integrity and availability of information, in all its forms, are fundamental to the ongoing functioning and good governance of the Office of the Auditor General (OAG). Failure to adequately secure information and information assets increases the risk of operational and reputational losses from which it may be difficult for OAG to recover.

This information security policy outlines OAG's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of OAG's information and information systems.

The OAG is committed to a robust implementation of Information Security Management hence aims to ensure the appropriate confidentiality, integrity and availability of its data.

Information were largely sourced from the following references/websites:

- Approved Information Security Policy from other Supreme Audit Institutions
- http://www.govnet.gov.fj/policies/default.html Government Information Technology Policies
- CISCO
- SANS Institute

2 Purpose

The purpose of this policy is to set out the expectation of the OAG in regards to the appropriate use of information, assets and network infrastructure establishing a culture of openness, integrity and trust.

The OAG is committed to ensuring appropriate security for all information technology data, equipment, and processes in its domain by adapting to the following principles:

- Protecting the information and network structures against internal and external threats.
- Providing a minimum level of access between the information and users on a "need to know" basis.
- Adopting the policy to ensure that security of informations, information systems and network infrastructure.
- Conduct continuous risk assessment, risk analysis and management procedures to information and information systems
- Monitoring the logs and audit trails to ensure that information are protected against unauthorized access.

- Ensuring that users comply with the Information Security Policies and other OAG Policies, Crimes Decree and Code of Conduct pertaining to information and information systems.
- Protecting the users and OAG from any inappropriate use that would expose OAG to risks including virus attack, compromising of network systems and services and any other legal issues.
- Conducting awareness and trainings within OAG about the security policy

3 Scope

This policy applies to:

- All classified and unclassified information either owned by OAG or that OAG is responsible for, in either electronic form or physical.
- All information and communication technology including the networks, server desktop computers, portable and remote devices/media (e.g. laptops, USB sticks, smartphones).
- Any personal equipment connected to the OAG systems.
- All staff, contractors, consultants, clients and other stakeholders that uses OAG Information system (whether on OAG premises or remotely) including all personnel applied with third parties all referred in here as the term ‘’Users”.

4 Definitions and Acronyms

Define terms used in the policy and explain any acronyms, for example:

Policy Maker	Auditor General
Management	Approval of Executive Management Committee

5 Policy Maker

Auditor-General

6 Key Words

Access privileges	Access privileges refer to the level of access granted to a user to perform his/her job duties.
Accountability	Accountability means that people are responsible for their action. This can be achieved through audit trails and non-repudiation.
Antivirus	Anti-virus is software used to prevent, detect and remove virus or malware on desktop, laptops, servers or any other computing equipment/devices.
Assets	An economic resources which can be tangible or intangible and capable of being owned or controlled to produce value and that is held to have positive economic value.
Audit Trails	A security-relevant sequential record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Authentication	The act of verifying a claim of identity. It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).
Authorization	Determines what a subject can do on the system and happens right after identification and authentication.
Availability	Part of the Information Security Triad which means that information should be available when it is needed.
Awareness	The knowledge and attitude users have regarding the protection of the physical and, especially, information assets of OAG.
Backup	Refers to the technique of making copies of data so that these additional copies shall be used to restore the original data after a data loss event.
Change	Any alteration to original software, hardware, or other aspects of the data processing environment and its attached networks.
Change Management	The formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested, Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.
Classification	Assigning categories to assets on pre-set criteria. In Information Security classification is used to categorize information assets in terms of sensitivity to protect it from unauthorized access, use, disclosure, disruption, modification or destruction.
Clear Desk	A control to ensure that all users clear their desks at the end of each work day. This not only includes documents, ID Cards and notes, but also post-its and removable media.
Confidential Data	Generalized term that typically represents data classified as confidential, according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.
Compliance regulation	The act of adhering to, and demonstrating adherence to, a standard or
Confidentiality	Part of the Information Security Triad; confidentiality means the non-disclosure of certain information assets expect to an authorized person as per the classification level of that asset.
Encryption	The conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Evidence	Everything that is used to determine or demonstrate the truth of an intrusion or breach to an information system.

Third Party	Individual or Entity having contractual agreement/obligations or legal agreement/obligations or business obligations to provide services to the OAG.
Information	Depicts any government related information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.
Information Assets	Any information or information processing facility that has value to the OAG.
Information Security	The act of protecting information that shall exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.
Information Assets	Definable pieces of information in any form, recorded or stored on any media that is recognized as “valuable” to OAG.
Information systems	Any computerized system used for managing and processing any government related information within a single entity or crossing multiple entities.
Integrity	Part of the Information Security Triad; integrity means that data cannot be modified without authorization, intentionally or unintentionally.
Institutional Data	All data owned by OAG
Key	A piece of information or a parameter that determines the functional output of a cryptographic algorithm or cipher. Key is used to de-crypt the encrypted information or data.
Logs	Stream of messages in time-sequence often comprises a log. Logs are generated by network, security devices, operating systems, applications and any computing device.
Malware	A software used or created to disrupt computer operation, gather sensitive information, or gain access to computer systems.
Offensive sites	Include sites that support derogatory religious sentiments, racism, offensive language, defamation, abusive attacks on any individual or group and sites have pornographic contents.
Patch	A piece of software designed to fix problems or improve the usability and performance of a system.
Policy	An Information Security related document written and maintained to provide governing statements regarding any Information Security key process, through setting the rules for expected behavior by users, systems administrators, management, and security personnel; authorize security personnel to monitor, probe, and investigate; define and authorize the consequences of violation; define the entity consensus baseline stance on security; help minimize risk; and help track compliance with regulations and legislation.

Recovery	Data recovery is the technique of recovering data from the backed up media in the event of loss or failure of data in the information processing systems.
Remote Access	The ability to connect to and access the OAG Infrastructure from a remote location using the virtual private network (VPN) of the OAG.
Retention period	The period for which an information / data needs to be stored and maintained before disposing it in a secured manner.
Risk	The quantifiable likelihood of potential harm that shall arise from a future event.
Risk assessment	A step in the risk management process to determine the qualitative and quantitative value of risk in relation to a recognized threat.
Security breach	An act that bypasses or contravenes security policies, practices or procedures.
Security control	Are safeguards or countermeasures to avoid, counteract or minimize security risks. They could be preventive, detective or corrective.
Spyware	A type of malicious software installed on computers that collects information about users without their knowledge.
SSID	Service Set Identifier (SSID) is a unique name set to a wireless local area network (WLAN) for the purpose of identification.
Threat	The expressed potential for the occurrence of a harmful event such as an attack. It could be any party with the intent and capability to exploit vulnerability in an asset such as a malicious hacker or a disgruntled staff.
URL	Uniform Resource Locator. Also termed as a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
User	All staff, contractors, consultants, clients and other stakeholders that uses OAG information and informations systems (whether on OAG premises or remotely) including all personnel applied with third parties.
VPN	A virtual private network or VPN is a network that uses a public network, such as the Internet, to provide remote offices or individual users with secure access to their OAG's network in a cost-effective manner.

7 Policy Management

The Information Security Policy is approved by the Auditor General and the Executive Management however advise and opinions will be provided by the IT Unit, IT Audit Group and users.

Monitoring and compliance of the policy is the responsibility of the Head of IT, Finance, People Management and Operations.

8 Confidentiality Agreements

All users are responsible to comply with the Policy. Users of OAG information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (***Annexure 21***). The agreement shall include the following statement, or a paraphrase of it:

I understand that any unauthorized use or disclosure of information residing on the OAG information resource systems may result in disciplinary action and/or termination of employment.

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing OAG information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

9 Security Team

The Security Team will be responsible for identifying areas of concern within the OAG and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the Auditor General and the term of each member appointed from each group will be at the discretion of the Auditor General or Deputy Auditor General.

The Security Team will provide a report to the Executive Management Committee on a quarterly basis or as determined by the Auditor General.

The Security Team (ST) will be made up of the following staff:

Position
Deputy Auditor General (Chairperson)
Head of IT, Finance, People Management and Operations
Senior Manager System Analyst and Data Analytics
System Administrator & Network Administrator
Risk and Compliance Officer
Representative – Financial Audit Group 1
Representative – Financial Audit Group 2
Representative – Performance Audit Group

10 Responsibilities of the Security Team will include but not limited to:

- Meeting monthly to discuss security issues and to review concerns that arose during the quarter.
- Identify areas that should be addressed during annual training and review/update security policies as necessary.
- Address security issues as they arise and recommend and approve immediate security actions to be undertaken.
- Identify areas of concern and act as the first line of defense in enhancing the security breach incident reporting mechanism of the OAG.
- Responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.
- Organise and facilitate trainings related to the security of information/records, any procedural changes and/or amendments to this policy.

11 System and Network Administrator

Responsibilities of the System and Network Administrator will include but not limited to:

- Maintain a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by the OAG. This log will be reviewed during the quarterly meetings of the Security Team.
- Twice yearly to audit the user login IDs and submit report to Executive Management Committee through the Deputy Auditor General and Head of IT, Finance, People Management and Operations to revoke all inactive logons.
- Reset password of users with logon IDs being locked or revoked.

12 Individual Users

It is the responsibility of the users who have been provided with the IT services and privileges (such as: domain user accounts, internet access, email account, and/or laptop etc) to make themselves aware of the policy and sub-policy statements and their responsibilities towards complying with it.

Users will be accountable for their actions.

13 Compliance and Breaches

This outlines the process for notifying affected users of a breach of protected information under this policy and/or state breach notification purposes.

13.1 Reporting a Possible Breach

a) Any employee who becomes aware of a possible breach of privacy involving confidential information in the custody or control of the OAG will immediately inform their immediate supervisor/manager.
b) Notification should occur immediately upon discovery of a possible breach however, in no case should notification occur later than twenty-four (24) hours after discovery.
    i. The supervisor/manager will verify the circumstances of the possible breach and inform the Assistant Auditor General within twenty-four (24) hours of the initial report.
    ii. Provide the Assistant Auditor General with as much detail as possible.
    iii. Be responsive to requests for additional information.
    iv. Be aware that the Assistant Auditor General or any authorised person(s) has an obligation to follow up on any reasonable belief that confidential information has been compromised.
c) The Assistant Auditor General, in conjunction with the Deputy Auditor General will notify the Auditor General as appropriate by taking into consideration the seriousness and scope of the breach.

13.2 Containing the Breach

The Assistant Auditor General or any authorized person(s) will take the following steps to limit the scope and effect of the breach.
Work with the Audit Group(s) or Corporate Services Group to immediately contain the breach. Examples include, but are not limited to:

i. Stopping the unauthorized practice

ii. Recovering the records, if possible
iii. Shutting down the system that was breached
iv. Mitigating the breach, if possible
v. Correcting weaknesses in security practices
vi. Notifying Executive Management Committee if the breach involves, or may involve, any criminal activity.

13.3 Investigating and Evaluating the Risks Associated with the Breach

To determine what other steps are immediately necessary, the Security Team will investigate the circumstances of the breach, determine root causes, evaluate risks, and develop a resolution plan which should be submitted to the Auditor General within five working days.

13.4 Prevention

a) Once immediate steps are taken to mitigate the risks associated with the breach, the Security Team will investigate the cause of the breach.
   i. If necessary, this will include a security audit of physical, organizational, and technological measures.
   ii. This may also include a review of any mitigating steps taken.
b) The Security Team will assist the responsible group to put into effect adequate safeguards against further breaches.
c) Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
d) The resulting plan will also include audit recommendations, if appropriate.

13.5 Compliance and Enforcement

All users are responsible for enforcing these procedures. Compliance with OAG Information Security policy is mandatory for all users. Failure to comply with this policy will result in disciplinary action under the terms and conditions of the contract of employment (OAG Disciplinary Policy), or engagement or prosecution under the Crimes Decree 2009.

14 Supporting Procedures/Guidelines

The guidelines to the policy are attached as Annexure I to this policy. This information will provide the background to the development of the policy should Officers need clarification.

RESPONSIBILITIES	
Implementation	IT Unit are responsible for implementing the policy.
Compliance	All users are responsible for complying with the policy.
Monitoring and Evaluation	Head of IT, Finance, People Management and Operations are responsible for monitoring and evaluating the policy.
Development and/or Review	Head of IT, Finance, People Management and Operations are responsible for developing and/or reviewing the policy.
Interpretation and Advice	Head of IT, Finance, People Management and Operations & Network and System Administrator are responsible for interpreting and advising on the policy.

15 Summary

The Information Security Policy is a set of policies to ensure that all information technology users within the domain of OAG and its networks comply with the rules and guidelines related to the security of the information stored digitally or within the OAG's boundaries of authority.

Supporting policies have been developed to strengthen and reinforce this policy statement. All users are required to familiarize themselves with these supporting documents and to adhere to it.

ANNEXURE 1 - Acceptable Use Policy

This policy defines the acceptable use of equipment and computing services, and the appropriate security measures that users should take to protect OAG resources and information. Inappropriate use exposes OAG to risks including compromises to the network systems, virus attacks and legal issues.

1.0 Usage of Information Technology Equipment

Purpose

- Outline the acceptable use of Information Technology (IT) equipment.
- To ensure that users follow an appropriate level of responsibility to safeguard the IT equipments in their custody and in the event of a loss, the only impact to the Office is the loss of equipment value and not the confidential and valuable information residing in it.

Policy

1.1 Acceptable Use and Ownership

a) Users shall report any suspicious activity observed on the OAG's Information Systems to the IT Unit immediately.
b) The IT Unit reserves the right to check network and systems on a periodic basis to ensure compliance with the IT Security Policy
c) Software installations on the laptop computers shall be in compliance with the approved and supported software services
d) Operating System and Application must be continuously updated with latest patches/service packs.
e) Only authorised personnel shall have access to information stored on Intranet servers or shared folders.
f) Classified data and files shall be maintained in accordance with the Information Classification Policy. (Refer to Annexure 10)

1.2 Handling Confidential Information

a) OAG has classified its information as defined in the Information Classification Policy (Annexure 10).
b) OAG would like to ensure that information assets are safeguarded at all times and that users will take all necessary steps to prevent unauthorised access to this information.
c) Authorised users are responsible for the security of their passwords and accounts.
d) Information contained on laptop is vulnerable hence special care should be exercised. Users must safeguard their laptop against loss, theft or damage and must not leave their laptops unattended especially in public areas.
e) All computers used by the user that are connected to the OAG Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database as per Anti-virus Policy. (Refer to Annexure 2)
f) Users must ensure that the anti-virus program is updated on their laptop all the time.
g) Users must continually backup all organizational related files stored on the laptop (monthly basis).

2.0 Email Usage

Purpose

- Ensure the appropriate method to use e-mail within OAG and with customers/clients.
- Ensure that risk of exposures of information and information assets are minimized.

Policy

2.1 Email Access

a) E-mail access will be provided to the user when joining the OAG and will be withdrawn when the user leaves OAG.
b) OAG e-mail will be used only for the conduct of OAG official and unofficial functions, and business needs.
c) Ensure that when sending email with the OAG information and attachments, the email recipient is the intended person to receive it.
d) Use of e-mail services for purposes constituting clear conflict with OAG's functions or in violation of OAG's e-mail policy is explicitly not allowed.
e) Users are not permitted to use the OAG email to participate in chain letters, junk emails, advertisements or unauthorised solicitations.
f) Users are not allowed to send large attachments containing graphics/pictures/objects/video files that can result in the disruption of the OAG's e-mail services unless if work related.
g) All users must scan and verify that the files to be sent via e-mail as attachments contain no viruses or malicious codes.
h) Use of e-mail services to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libelous is strictly prohibited.
i) Sending emails from another user's email account is not permitted.
j) Users are not allowed to send sensitive information to personal email accounts.
k) It is strictly prohibited to use auto forwarding of confidential emails to personal email accounts unless this has been discussed and approved by Immediate Supervisors.

2.2 Storage Limits

a) All mailboxes will have a maximum storage limit of 4GB – 5GB for Executive Management and 1GB for all other employees.
b) Size of email attachment is restricted to 10 - 15MB and regular file splitting and compression can be used to keep within these limits.
c) Requirement for a large email or mailbox size will need to go through the approval process of line managers and Assistant Auditors General.

2.3 Email Retention

All emails will be deleted after 60 days. If a user has sufficient reason to keep a copy of an email, the message must be archived.

3.0 Internet Usage

Purpose

- To ensure that all users have an efficient internet access within a secure network environment.
- To ensure communication within and outside the OAG network is secure.
- To manage user productivity and optimize the use of IT infrastructure through control of internet access.

3.1 Policy

a) Internet access will be provided for all staff of OAG and will be suspended when a user leaves OAG.
b) Ensure that the internet is used for official, research and development purposes only.
c) Users are permitted with limited personal use of the internet as long as:
    i. It does not delay the OAG operations and functions
    ii. It does not violate the applicable laws or OAG policy and it does not interfere with the network performance
    iii. Users are not allowed to share their login identification (ID) and password when accessing internets
    iv. Accessing, contributing and downloading from offensive sites are strictly not allowed. Offensive sites include sites that support derogatory religious sentiments, racism, offensive language, defamation, abusive attacks on any individual or group and sites having pornographic content.
d) Users are not allowed to download software from the internet and install it on computer equipment's as it may contain viruses.
e) Users are not permitted to use internet access to transmit confidential, political, obscene, threatening or harassing materials.
f) Users are not allowed to represent themselves as another person over the internet.
g) Users are not allowed to use any automated tools or any other means for gaining unauthorised entry into third party systems or any resource over the internet to which they do not have authorised access rights.
h) Users are not allowed to change the browser settings to use any third party proxy server or external Virtual Private Network (VPN) server to connect to the internet.
i) The OAG has all the rights to enforce Uniform Resource Locator (URL) filtering to block access to certain sites and limit the bandwidth on certain sites or application that are considered offensive or not relevant to the organization.

ANNEXURE 2 – Anti Virus Policy

This Policy provides the instructions on measures that must be taken by users to help achieve an effective virus detection and prevention.

Purpose

- To detect, prevent and minimize the impact of virus outbreaks in OAG systems such as servers and end-user laptops.
- To define appropriate control measures for users in order to protect the systems against virus attacks.
- To ensure protective and optimum performance for the users when using the systems without any considerable delay.

Policy

2.1 Scanning for Virus

a) All files and software downloaded or received from external networks, e-mail, or on any other medium such as data storage media should be first scanned for viruses, malicious code prior to its use.
b) File servers shall be scanned for viruses on a regular basis.
c) Any data storage media brought into the OAG must be scanned for virus before being used by the user.
d) OAG users with computing equipment shall update the Anti-virus software with the latest updates.

User Responsibilities

a) Anti-virus software will be configured to clearly instruct the user to either disinfect or erase the file if a virus is found and users should not disable, remove or change the configuration of the Anti-virus software installed on their laptops.
b) All users are advised to report virus attacks if any detected to the IT Unit.
c) All users are not allowed to open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these emails along with the attachments immediately and then empty the Recycle Bin.
d) All users must delete spam, chain, and other junk email without forwarding.
e) On receiving a virus alert or noticing suspicious activity, users are advised to immediately disconnect their systems from the network and contact IT Unit for immediate support.
f) The IT Unit will inform the users regularly of the latest viruses and the precautions to be taken by the users to mitigate the virus risk. (Refer to Annexure 14 Security Awareness and Training Policy)
g) The IT Unit will regularly check the Anti-virus server logs to see if all the laptops and servers are running with the latest updates, if not, this should be manually done.
h) All critical security updates, as soon as they are received from the vendors, will be rolled out to the various laptops and servers.
i) Shareware is not to be used, as it is one of the most common infection sources. If it is absolutely necessary to use shareware, it must be authorised by the Auditor General after it has been vetted by the IT Unit.
j) All Users (except the IT Unit) are prohibited from running executable files (these are files ending with .EXE and .COM extensions).

ANNEXURE 3 – Back-up and Restoration Policy

This policy defines the backup and restoration standard for all OAG information and information systems.

Purpose

To ensure data recoverability in the event of accidental data deletion, corrupted information or an unplanned business disruption that could cause damage to data integrity, confidentiality and/or availability.

Policy

3.1 Backup Requirements

a) Backup requirements for all information and information systems within the OAG must be identified and documented.
b) The IT Unit will record and maintain the backup requirements for all systems under the responsibility of IT at a minimum, this will include details of backup frequency, information to be backed up, storage media, retention and recycling.
c) In the case of data stored locally on laptops, it will be the responsibility of the users to ensure that the data is backed up on a periodic basis, preferably by connecting to the OAG network and synchronizing the data between the laptops and the network data storage created specifically for each staff. (Refer to Annexure 8 on the Data Storage Policy)
d) The IT Unit will decide which information is to be backed up and the frequency of backups in consultation with the information owner based on the system criticality and it's Recovery Time. The production and operation of the IT systems, databases and networks must be implemented in such a way that it does not rely upon any single person. Strategies must be implemented to ensure strong human resource capacity building and backup policy.

3.2 Backup Schedules

All systems software, application software, user data, database information and associated documentation, will be backed up on a regular basis to facilitate recovery in the event of an unplanned system disruption.

The frequency of the backup will be at a minimum:

a) System Software: Before and after any changes to systems such as an upgrade, changes in configuration, patch updates etc.
b) Application Software: Before and after any changes to the application such as a new version release or modification to application source code.
c) User Data or Database Information: On a periodic basis (Daily / Weekly / Monthly), based on the backup frequency identified for the individual systems.
d) Device Configurations: Before and after any changes to the configurations of critical devices such as Routers, Firewalls, switches etc.
e) Documentation: Latest copies of system documentation (e.g. Technical reference manuals, User manuals etc.) will be backed up and maintained.

3.3 Performing Backups

a) IT Unit will maintain a weekly backup checklist specifying the various backups that are required to be taken for that day.
b) The weekly backup operations will be logged against the checklist reviewed and signed off by the assigned staff at the end of the day. At a minimum, the backup log will record details about the backup carried out, start and end time, identification of the media used and success or failure status.
c) Any unscheduled or one-time backups will require specific authorization of the Deputy Auditor General. This will also be recorded in the daily backup list with appropriate reasons for the same.
d) The backup checklist will be independently reviewed by Head of IT, Finance, People Management and Operations periodically.

3.4 Backup storage

a) Backup media will be stored in two different locations - one onsite within the OAG's premises, and the other at a location approved by the Executive Management Committee.
b) Physical access to the backup media will be adequately secured by implementing appropriate controls.
c) Physical access to the backup storage locations will be restricted only to authorized personnel.
d) A physical access log will be maintained for recording access to the backup storage locations.
e) This will be reviewed on a periodic basis by Head of IT, Finance, People Management and Operations.

3.5 Testing and Restoring

a) The ultimate goal of any backup process is to ensure a restorable copy of data exists on the backup media. As a result, it's essential to regularly restore the data from backup media. Full restore will be performed according to the annual restore plan. These plans will be reviewed by IT Unit on a regular basis.
b) Data will be restored if:
    i. There is a compromise of the system / device.
    ii. Files have been corrupted, deleted, or incorrectly modified but try to recover.
    iii. The information to be accessed is located in an archive backup.
c) In the event a data restore is desired or required, the following policy will be adhered to:
    i. An approval from the data owner is needed for any restoration process.
    ii. An approval from the Deputy Auditor General is also required for any restoration process.
d) In the event of a local data loss due to human error, the affected end user shall contact the IT Unit and request a data restore.

ANNEXURE 4 – Change Management Policy

To increase awareness and understanding of proposed changes across OAG and ensure that all changes are made in a thoughtful way that minimize negative impact to OAG and our stakeholders.

Purpose

To ensure change requests comply with OAG change management procedures and eliminate/reduce the number of errors related to change planning and implementation.

4.1 Policy

It is the responsibility of the IT Unit to manage the life cycle of all IT systems supporting OAG operational activities.

To ensure effective change management within the OAG's IT environment, the following shall apply:

a) Under no circumstances shall any entity integrate new applications into a production environment without approval from the Auditor General.
b) All proposed types of changes that shall impact OAG's information resource must adhere to this Policy.
c) No change shall be made to the OAG IT environment without the approval of the Auditor General.
d) All changes shall follow the established approval process to ensure that changes are completed with minimum restrictions and risk.
e) All changes shall be well documented for future reference.
f) The IT staff authorised to implement the change to the system should ensure that all necessary data backups are performed prior to the change.
g) The IT staff authorised to implement the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

ANNEXURE 5 – Clean Desk Policy

To establish the minimum requirements for maintaining a 'clean desk' – where confidential and critical information about OAG employees, OAG intellectual property, our clients and other stakeholders is secure in locked areas and out of site.

Purpose

- To ensure that all confidential materials are removed from a user workspace and locked away when the items are not in use. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace.
- To increase the user's awareness about protecting sensitive information.

5.1 Policy

a) Users are required to ensure that all confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be away from the office for an extended period.
b) Laptops and other IT devices must be locked when the office is unoccupied and completely shut-down at the end of the working day.
c) Confidential and restricted information must be removed from the desk and locked in the drawer when the desk is unoccupied for an extended period and at the end of the working day. This is especially important for permanent, payroll and personnel files.
d) Keys used for access to restricted information must not be left at an unattended desk.
e) Printouts containing confidential/restricted information should be immediately removed from the printer.
f) Upon disposal of confidential/restricted information, the documents should be shredded before it is placed in the disposal bins.
g) Whiteboards containing confidential/restricted information should be erased.
h) Treat mass storage devices as sensitive and secure them in a locked drawer.
i) All printers and fax machines should be cleared of papers as soon as they are printed, this helps ensure that confidential/restricted documents are not left in printer trays for an unauthorised person to collect.

ANNEXURE 6 – Data Access Policy

This Policy establishes measures for the protection, access and use of OAG institutional data stored in electronic and physical format.

Purpose

Defines the responsibilities of who can access and manage the institutional data.

Institutional data — Consists of information stored in any OAG databases or on paper that contains information related to OAG operations. All institutional data whether maintained in the central database or copied into other data systems, remain the property of OAG and are governed by this policy.

Policy

6.1 Institutional Data Use

a) To be used only for appropriate business of OAG. Data shall be used only as required in the performance of job functions.
b) Under no circumstances shall any user use personally identifiable private/confidential institutional data in any publication, seminar, or professional presentation, or otherwise release data, in any form, outside the OAG without prior written approval from the appropriate data steward.
c) Data must never be left on any system to which access is not controlled (USB drive, computer hard drive).
d) For all machines (laptops/desktops) the USB ports access shall be deactivated through the Active Directory to prevent unauthorised downloading and sharing of sensitive data with the use of external portable drives. In addition, to avoid the risk of machines getting corrupted with malware like computer viruses, worms, Trojan horses and spyware.
e) Staff planning to download/upload data from any external portable drive for official purposes shall liaise with the IT Support Team.
f) Audit Managers shall be provided with encrypted USB to facilitate the transfer of audit files and documents that cannot be sent through email.
g) Institutional data (regardless of who collects or maintains it) shall be shared among those employees whose work can be done more effectively by knowledge of such information. Though the OAG must protect the security and confidentiality of data, the procedures to allow access to data must be adhered to at all times.
h) All users of institutional data have the right to expect the data to be accurate.
i) All who maintain institutional data have the responsibility to keep them accurate.

6.2 Categories of Data

Refer to Information Classification Policy on Annexure 10 for the categories of data.

6.3 Types of Access

Query-only Access

a) Access enables the user to view, analyse, and download, but not change institutional data.

b) Once information is downloaded, data can but should not be altered in word processing documents or spreadsheets. Downloaded information should be used and represented responsibly.

Maintenance Access

a) Maintenance access provides both inquiry and update capability. Maintenance is defined as add, delete and change. This capability is generally limited to the users directly responsible for the collection and management of the data.
b) Access is available to administrators and users who have an authorized need to change institutional data in the routine performance of their job duties.
c) Each user of administrative information is assigned appropriate combinations of query-only and maintenance access to specific parts of the administrative information system. The types of access are determined by the data stewards (Definition provided below).

6.4 Data Ownership

Data stewards will be appointed to manage specific elements of institutional data.

Data Stewards

a) Data steward responsibilities are central for maintaining OAG operations.
b) Should identify a backup.
c) Responsible for ensuring the accuracy, completeness, integrity, and as appropriate, the confidentiality of OAG information.
d) To provide training to other users with respect to access and manipulation of institutional data.
e) May make data available to others within his or her group/team/division for use and support of the group/team/division's functions.
f) Shall define access control principles and restrictions on use and handling for the data for which they are assigned responsibility, consistent with data categorization described in Annexure 10.
g) Before granting access to data, the data steward shall be satisfied that protection requirements have been implemented and that a "need to know" is clearly demonstrated. By approving end-user access to institutional data, the data steward consents to the use of this data within the normal business functions of OAG.
h) Access to OAG data shall not be granted to persons unless there is an established "need to know".
i) Required to review all security authorizations at least annually for their area and make additions or deletions as necessary.

The data stewards for the OAG are as follows:

Area	Steward
Registry	Registry Clerk
Payroll	Payroll Officer
Finance Department	Senior Accounts Officer
IT Server Room	System and Network Administrator
Shared drives for Groups	Audit Managers
Shared drives for Executive Management	Senior Secretary
Shared drives for WP	Registry Clerk
Shared drives for Committee Folders	Elected Secretary (for the term)
Shared drives for Permanent Files	Senior Auditors / Audit Managers

Information Supervisors

a) All levels of administrative management shall ensure that, for their areas of accountability, each information system user knows his/her responsibilities as defined in this policy.
b) Supervising administrators shall ensure a secure office environment with regard to all institutional information systems.
c) Supervising administrators shall validate the access requirements of their staff according to job functions, before submitting requests for the provision of access.

Users

a) Each user is responsible for all transactions occurring during the use of his/her login and password. Refer to Annexure 12 on Password Management Policy.
b) Users are responsible for understanding all data elements that are used otherwise the user to consult the appropriate data steward or his/her immediate supervisor.
c) Users must exercise due care in using the institution's electronic information systems, to protect data files from unauthorized use, disclosure, alteration, or destruction.
d) Each user is responsible for security, privacy, and control of his/her own data.
e) May not disclose data to others, except as required by their job responsibilities
f) Must not use data for their own personal gain, nor for the gain or profit of others
g) Must not access data to satisfy their personal curiosity
h) Must not use institutional data (in detail or summary) in any publication, seminar or professional presentation without permission of the OAG Executive Management unless if it is work related.
i) Also refer to Annexure 15 User Access Management Policy

IT Unit

a) To ensure that a variety of security measures are in place.
b) Maintain the central institutional database and ensure data security, integrity, and availability to all who have been granted access to it.
c) Perform database system backup on a regular basis. Refer to Annexure 3
d) A disaster recovery plan will focus on minimizing the disruption caused when the central computing facility is inoperative. Refer to Annexure 9
j) The cost of data protection to commensurate with the value of data and the legal implications of the loss of such data.
k) To process requests for data access through data stewards and serve as the initial point of conflict resolution in instances where requests for access conflict with this policy.

ANNEXURE 7 – Database Management Policy

This policy addresses the operating policy that focuses on the management and governance of data assets.

Purpose

The database management policy establishes methods for protecting databases from accidental or malicious destruction of data or damage to the database infrastructure.

7.1 Policy

a) Default service account passwords must be changed after creation. All default operating system account passwords must be changed. (Refer to Annexure 12 on the Password Management Policy)

b) The IT Unit shall have the operating system privileges to create and delete files in the production servers. Access to non-production database servers must be approved by Deputy Auditor General or Assistant Auditors General.

c) Each database service account is managed by a single employee. During vacations and emergencies, these accounts must be delegated to other users temporarily based on the Deputy Auditor General or Assistant Auditors General's approval.

d) All database user account access must be approved by the Deputy Auditor General or Assistant Auditors General. The approval should include the requesting department manager, data owner, and Deputy Auditor General or Assistant Auditors General. The access for all accounts must be reviewed once every quarter to ensure users have access as per their current job role.

e) No database user accounts associated with an employee shall have direct privileges to update, create or delete records in the production databases. Database Roles (based on job title and responsibilities) should be used to manage the privileges available to users.

f) All database user accounts will be associated with a password policy as per the Password Management Policy (Annexure 12).

g) Data auditing mechanisms must be in place to investigate in case of unauthorized activities on the database.

h) Live production systems data must be updated from the relevant front-end applications by the appropriate authorized users. Any scripts or back-end changes to production databases must have approvals from data owner and Deputy Auditor General or Assistant Auditors General.

ANNEXURE 8 – Data Storage Policy

Access and use of network storage establishes an obligation on the part of the individual to use this resource as defined in this policy.

Purpose

- This policy will assure network data storage is used in an acceptable manner to maintain network availability and performance.
- The IT Unit is responsible for managing network storage which includes daily backups, securing access, monitoring, and reporting of usage patterns.

Policy

8.1 Appropriate File for Storage

a) Files that directly pertain to the operations of OAG shall be saved on a server. These include audit files, payroll, human resource and other correspondences pertaining to the operations of OAG.

b) Users are not allowed to store any personal or non-business related files on storage server.

8.2 Storage Space Allocation

Alerts will be sent to all employees who are close to exceeding their server space quota. If an employee exceeds their server space quota, they will be unable to save files until sufficient allocated space is freed in order to accommodate them. If an employee needs support in freeing storage space, he or she shall contact the IT Unit.

8.3 Tips for Conserving Storage Space

a) It is the responsibility of every user to ensure that they use their server storage space allocation wisely.

b) Each user should set aside time on a monthly basis to ensure that they remain within their space quota.

c) Identify, remove and/or archive items that are:

   i. Outdated, such as preliminary draft versions of current documents.

   ii. Out-of-use or orphaned files.

   iii. Duplicated files.

   iv. Non-business related or non-critical files

ANNEXURE 9 – Disaster Recovery Plan Policy

This Policy is to ensure that there are plans in place to restore the operability of designated systems and applications at the OAG should there be any disaster or disruption.

Purpose

The purpose of this policy is to establish a well prepared strategy to avoid potential threats, promptly responding to situations that threatens the information and information systems for OAG and identifying resources and strategies for recovery.

Policy

a) The Disaster Management Team shall be responsible for developing and regularly updating the written disaster recovery plan for the purpose of:

i. Restoring or recovering any loss of confidential data/information and/or systems necessary to make audit and non-audit information available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

b) The disaster recovery plan shall include the following:

iii. Current copies of the information systems inventory and network configuration developed and updated as part of OAG's risk analysis.

iv. Current copy of the written backup procedures developed and updated pursuant to this policy.

v. An inventory of hard copy forms and documents needed

vi. Identification of an emergency response team. Members of such team shall be responsible for the following:

1. Determining the impact of a disaster and/or system unavailability on OAG's operations.
2. In the event of a disaster, securing the site and providing ongoing physical security.
3. Retrieving lost data.
4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
5. Taking such steps necessary to restore operations.

vii. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of OAG's risk analysis

viii. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

1 Members of the immediate response team.
2 Facilities at which backup data is stored.
3 Information systems vendors.
4 All current workforce members.

c) The disaster recovery team shall meet on at least an annual basis to:

i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by OAG.
ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills.
iii. Review the written disaster recovery plan and make appropriate changes to the plan.

(Refer to the OAG Disaster Recovery Plan for detail information)

ANNEXURE 10 – Information Classification Policy

This Policy is concerned with the management of information to ensure information is handled well with respect to the threat it poses to OAG. It is not the purpose of this policy to create unnecessary restrictions to data access or to impede use for those individuals who use the data in support of OAG mission and visions. This policy serves to assure staff that the expectation of privacy and confidentiality of their data will be maintained.

Purpose

To establish a framework for classifying and handling data based on its level of sensitivity, value and criticality to OAG. Classification of data will aid in determining baseline security controls for the protection of data.

Policy

All staff have a responsibility to protect the confidentiality, integrity, and availability of data irrespective of the medium on which the data resides and regardless of format such as, but not limited to: electronic, paper and any other physical form.

OAG shall classify its data based on its level of sensitivity and the impact to the OAG should that data be disclosed, altered or destroyed without authorisation.

Categories of Data

All OAG data shall be classified into one of the three categories:

Categories	Description
Confidential	• Due to its nature, requires more control with respect to access or disclosure. • Confidential information may be accessed by OAG personnel with a legitimate need-to-know, based on their role within the OAG, or as authorised by the Executive Management Committee. • Disclosure of confidential data outside OAG will take place only with the advance authorisation of the relevant data steward and approval by the *Auditor General*. • To be stored on network servers in a secure environment. • Must not be downloaded or saved to desktop computers or laptops unless that computer is encrypted. Even deleted files can be recovered and accessed using inexpensive data recovery tools. • Must not be downloaded and stored on USB drives or other peripheral devices without that device being properly encrypted. Encrypted USB devices to be provided by the IT Unit. • Must not be transferred via email, file transfer protocol (FTP) or any other network application without being encrypted. • Printed reports containing confidential data must be kept secure and should be properly disposed of via shredding when no longer

Categories	Description
	needed. Each user is responsible for security, privacy and control of the confidential data in their possession. • Data restricted by law or decided by OAG Executive Management as high risk data. • The unauthorised disclosure, alteration or destruction of that data could cause a significant level of risk to OAG operations and reputation. • The highest level of security controls should be applied.
Internal data	• Because of its highly sensitive nature or because of legal restrictions, requires strict access control and limited disclosure. • May be accessed by OAG personnel with a legitimate need-to-know, based on their role within the OAG or as authorised by their supervisor or the appropriate data steward. • Disclosure of private information outside the OAG or to those not authorised by the Executive Management Committee will not be allowed, however any disclosure of private information will be made only with advance authorisation of the relevant data steward and approved by the *Deputy Auditor General or the Assistant Auditors General*.
Public data	• Information or data that may be freely accessed or disseminated at the discretion of the OAG Executive Management Committee. • Examples include press releases, OAG Magazines, Policies and Annual Reports published in the OAG websites.

ANNEXURE 11 – Log Management Policy

Change management logs document all changes made to technologies used with OAG. Logs are records of events that occur within the information systems and an invaluable resource used to optimize systems and networks, establish baselines, perform audits and assist with regulatory compliance.

Purpose

In conjunction with appropriate tools and procedures, audit trails can validate individual accountability, a way to reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance. The need to audit individual accountability, reconstruct events, detect intrusions, identify problems and demonstrate regulatory compliance emphasizes the need for organization's to develop an effective log management strategy to generate, analyse, store and dispose of log data.

Policy

a) The IT Unit shall create, maintain and implement a secure log management infrastructure by balancing system performance, storage resources, and legal requirements.

b) Commit resources to perform timely log review to identify and analysis access, change monitoring, malfunction, resource utilization, security events and user activity

c) Identify roles and responsibilities of staff associated with this process.

d) Develop standards, procedures, and guidelines as needed to support this program.

e) Make the system available for applications that need log management and analysis capabilities.

f) The system should log: User ID, Dates and times of logon and logoff, terminal identity (if possible) and network address (if possible), unsuccessful system or data access attempts (if possible), system alerts or failures or other significant events as appropriate.

g) Special treatment should be performed for administrator, super-user or other privileged access.

11.1 Log Retention

a) Log retention has to be done according to legal requirements, targets, guidelines and security policies of OAG.

b) In the course of running different services on the server a number of logs are collected, like web logs, email logs, system services logs, applications logs and security logs. These logs can take many different formats e.g. text, word, excel, notepad files and email format.

c) Many of the above documents can be retained either on paper records or in electronic form. Retention of specific documents shall be necessary to:

   i. Fulfill statutory or other regulatory requirements.

   ii. Provide evidence for an events, agreements in case of disputes.

   iii. Meet operational needs.

   iv. Ensure the preservation of logs of historic or other value.

d) Conversely, the permanent retention of all logs is undesirable, and appropriate disposal is to be encouraged for the following reasons:

   i. Shortage of storage space.

   ii. Disposal of existing logs can free up space for more productive activities.

   iii. Indefinite retention of personal data shall be unlawful.

   iv. Reduction of fire risk (in the case of paper records).

11.2 Log Retention and Protocol

a) Logs should be enabled for operating system, applications, firewall, switches and other security devices in the data center as defined in the log management policy.

b) Logs should be saved locally on the devices, logs are collected for the period of one week, after which logs will be transferred to centralized network storage.

c) The entire log should be reviewed by IT Unit for any malicious activity or at least manually once a year.

d) The retention period for the logs should be 1 year.

e) After the completion of retention periods logs should be disposed securely.

f) IT Unit is responsible to handle all the issues related to logs.

g) Logs can be used to address performance issues for the servers, applications, firewall, router or other devices.

h) Log deletion should be authorised by the Deputy Auditor General, where computer files are concerned.

i) Paper records related to logs must be shredded on site with the approval of the Deputy Auditor General.

ANNEXURE 12 – Password Management Policy

Passwords are an important aspect of computer security to protect the confidentiality, integrity and availability of information, systems, services and applications within the OAG network.

Purpose

- Enforce adequate password controls in the systems and at the user level.
- Ensure that only authorised users can access certain information, applications, services and systems.

Policy

a) Every user is provided with a login ID and a password to access the systems, applications, email and network infrastructure.

b) Access will be withdrawn when the employee leaves the OAG.

c) All access and security codes such as passwords, Personal Identification Numbers ("PINs") and security tokens are considered as confidential information and must be protected and handled accordingly.

d) Users must protect passwords at all times against disclosure or unauthorized use, including when generated, distributed, used and stored.

e) Passwords must follow a minimum set of security requirements including password length, complexity, reuse, and age and account lockout after unsuccessful authentication(s). (**POL 39/2020 OAG Password Policy**)

f) Passwords for Privileged Accounts must follow stronger requirements than regular user passwords.

g) In addition to the guiding principles above, passwords must be created and managed in accordance with the guidelines contained in the **POL 39/2020 OAG Password Policy**.

ANNEXURE 13 – Physical Access to Server Room Policy

The objective of this policy is to establish the rules for accessing the OAG Server Room.

Access to Server Room

a) Door to the server room shall be closed at all times. Biometric shall be installed at the door to the server room to log access into the room.

b) Any access to the server room shall be logged (in and out, reasons, authorized by whom). In addition, all accompanying persons shall be listed.

c) Any non-OAG staff accessing the server room shall be accompanied by any of the OAG IT staff at all time.

d) Visitors are not allowed to bring phones or computer, except if permission has been provided by the Deputy Auditor General.

e) Access to server room during an emergency (apart from the authorised persons or IT staff), should be approved by any of the Executive Management Committee (Assistant Auditor Generals, Deputy Auditor General or the Auditor General)

Monitoring the Access

a) Any access and activity inside the server room shall be recorded.

b) CCTV shall be working and recording all motions in the server room.

c) Windows to the server room have to be clear all the time, so that at all times activities and persons in the server room can be easily identifiable.

ANNEXURE 14 – Security Awareness and Training Policy

This policy specifies an information security awareness and training program to inform and motivate users regarding information risk, security, privacy and related obligations.

Purpose

To establish a security awareness and training program for all OAG staff.

Policy

All staff shall receive appropriate training concerning OAG's security policies and procedures. Such training shall be provided on an ongoing basis to all new employees and security reminders to be disseminated on a regular basis (quarterly) for all employees.

Security Training Program

a) The System Network Administrator will be responsible for the development and delivery of initial security training. All staff to receive such initial training addressing the requirements of the Information Security Policy. Security training to be provided also to all new staff as part of the induction process. Attendance and/or participation in such training to be mandatory for all staff. The Talent Management Specialist (TMS) shall be responsible for maintaining appropriate documentation of all training activities.

b) The System Network Administrator will be responsible for the development and delivery of ongoing security training provided to all staff in response to environmental and operational changes impacting the security of information maintained at the OAG e.g., addition of new hardware or software, and increased threats.

Security Reminders

a) The System Network Administrator will generate and distribute to all staff routine security reminders on a regular basis (recommended quarterly). Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The System Network Administrator may provide such reminders through formal training, e-mail messages, and discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The System Network Administrator will be responsible for maintaining appropriate documentation of all periodic security reminders.

b) The System Network Administrator will generate and distribute special notices to all staff providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

ANNEXURE 15 – User Access Management Policy

Adequate security of information and information systems is a fundamental management responsibility. This Policy ensures that OAG has adequate controls to restrict access to systems and data.

Purpose

The purpose of this policy is to prevent unauthorised access to the information systems and to ensure the availability of information for authorised users.

Policy

The first line of defense in data security are the individual users. Outlined below are the mandatory requirements for all users.

New Users

a) Access to applications, databases, network, email and servers are controlled through a formal user registration process beginning with a formal notification from Corporate Services Group. Each user is assigned a unique user ID for identification and accountability purposes.

b) The IT Unit should ensure that all new users should be assigned their user ID and password.

c) The use of shared IDs is not permitted.

d) All users shall be responsible for the use and misuse of their individual logon IDs.

Change in User Roles

a) The People Management Specialist shall promptly notify the System Network Administrator of the change in roles so that the user has access to the minimum necessary data to effectively perform their new job functions.

b) The System Network Administrator should also be informed of the effective date of the position change so that the employee will have appropriate roles, access, and applications for their new job responsibilities.

Termination of User Logon Account

a) Upon termination of an employee, whether voluntary or involuntary, the Head of IT, Finance, People Management and Operations or an authorised staff shall facilitate the termination of logon account.

b) If an employee's termination is voluntary and employee provides notice, the People Management Specialists shall promptly notify the System Network Administrator of employee's last scheduled work day so that their user account(s) can be configured to expire.

c) Twice yearly, the Head of IT, Finance, People Management and Operations or an authorised staff shall provide a list of active user accounts for both network and application access, to the Security Team for review. The team shall review the employee access lists and if any of the employees on the list are no longer employed by the OAG, the IT Unit must be informed to immediately terminate the logon account.

ANNEXURE 16 – Bluetooth Baseline Requirements Policy

This policy defines the minimum baseline standard for connecting Bluetooth enabled devices to the OAG network or OAG owned devices.

Purpose

To ensure sufficient protection on OAG data with the use of Bluetooth and Bluetooth enabled devices.

Policy

a) When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where you PIN can be compromised.

b) If your Bluetooth enabled equipment asks for you to enter your PIN after you have initially paired it, you must refuse the pairing request and report it to IT Unit immediately due to a possibility of security vulnerabilities.

c) Use a minimum PIN length of 8. A longer PIN provides more security.

d) Switch the Bluetooth device to use the hidden mode (non-discoverable)

e) Bluetooth mode must be turned off when not in use.

f) Ensure device firmware is up-to-date.

g) OAG Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.

h) Bluetooth users must only access OAG information systems using approved Bluetooth device hardware, software, solutions, and connections.

i) Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.

j) Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to Immediate Supervisors and to the IT Unit.

The following is a list of unauthorized uses of OAG owned Bluetooth devices:

a) Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.

b) Using OAG owned Bluetooth equipment on non-OAG owned Bluetooth enabled devices.

c) Unauthorized modification of Bluetooth devices for any purpose.

ANNEXURE 17 – Remote Access Policy

Remote access to OAG network is essential to maintain OAG's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than the OAG network. While these remote networks are beyond the control of OAG we must mitigate these external risks to the best of our ability.

Purpose

- Define standards for connecting to the OAG's network from any remote host.
- Minimize the potential exposure to the OAG systems which shall result from unauthorised use of its resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image and critical internal systems.

Policy

a) It is the responsibility of the users with remote access privileges to the OAG network to ensure that their remote access connection is given the same consideration as the user's onsite connection to the OAG.

b) The user is responsible to ensure no one violates any of the organizations policies, does not perform illegal activities, and does not use the access for outside business interests of OAG when accessing the OAG network remotely. The user bears responsibility for the consequences should the access be misused.

c) Users with remote access privileges must ensure that the OAG-owned or personal computer or workstation, which is remotely connected to OAG's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

d) At no time should any user provide their login or email password to anyone, not even family members.

e) Users with remote access privileges to the OAG's network must not use personal email accounts (i.e., Hotmail, Yahoo, AOL, etc.), or other external resources to conduct the OAGs business, thereby ensuring that official business is never confused with personal business.

f) Personal device that is used to connect to the OAG network must meet the requirements of the OAG-owned equipment for remote access.

g) All hosts that are connected to the OAG network via remote access technologies must use the most up-to-date anti-virus software and patched appropriately, this includes personal computers.

ANNEXURE 18 – Router and Switch Security Policy

This Policy defines the security features used on OAG routers.

Purpose

To describes the required minimal security configurations for all routers and switches connecting to a production network or used in a production capacity at or on behalf of OAG.

Policy

Every router must meet the following configuration standards:

a. No local user accounts are configured on the router. Routers and switches must use Terminal Access Controller Access-Control Systems (TACACS+) for all user authentication.

b. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

c. The following services or features must be disabled:
   i. IP directed broadcasts
   ii. Incoming packets at the router/switch sourced with invalid addresses
   iii. User Datagram Protocol (UDP) small services
   iv. All source routing and switching
   v. All web services running on router
   vi. OAG discovery protocol on Internet connected interfaces
   vii. Telnet, File Transfer Protocol, and Hyper Text Transfer Protocol services
   viii. Auto-configuration

d) The following services should be disabled unless a business justification is provided:
   i. OAG discovery protocol and other discovery protocols
   ii. Dynamic trunking
   iii. Scripting environments, such as the Tool Command Language shell

e) The following services must be configured:
   i. Password-encryption
   ii. Network Time Protocol configured to a corporate standard source

f) All routing updates shall be done using secure routing updates.

g) Use corporate standardized Simple Network Management Protocol (SNMP) community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

h) Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

i) Access control lists for transiting the device are to be added as business needs arise.

j) The router must be included in the corporate enterprise management system with a designated point of contact.

k) Each router must have the following statement presented for all forms of login whether remote or local:

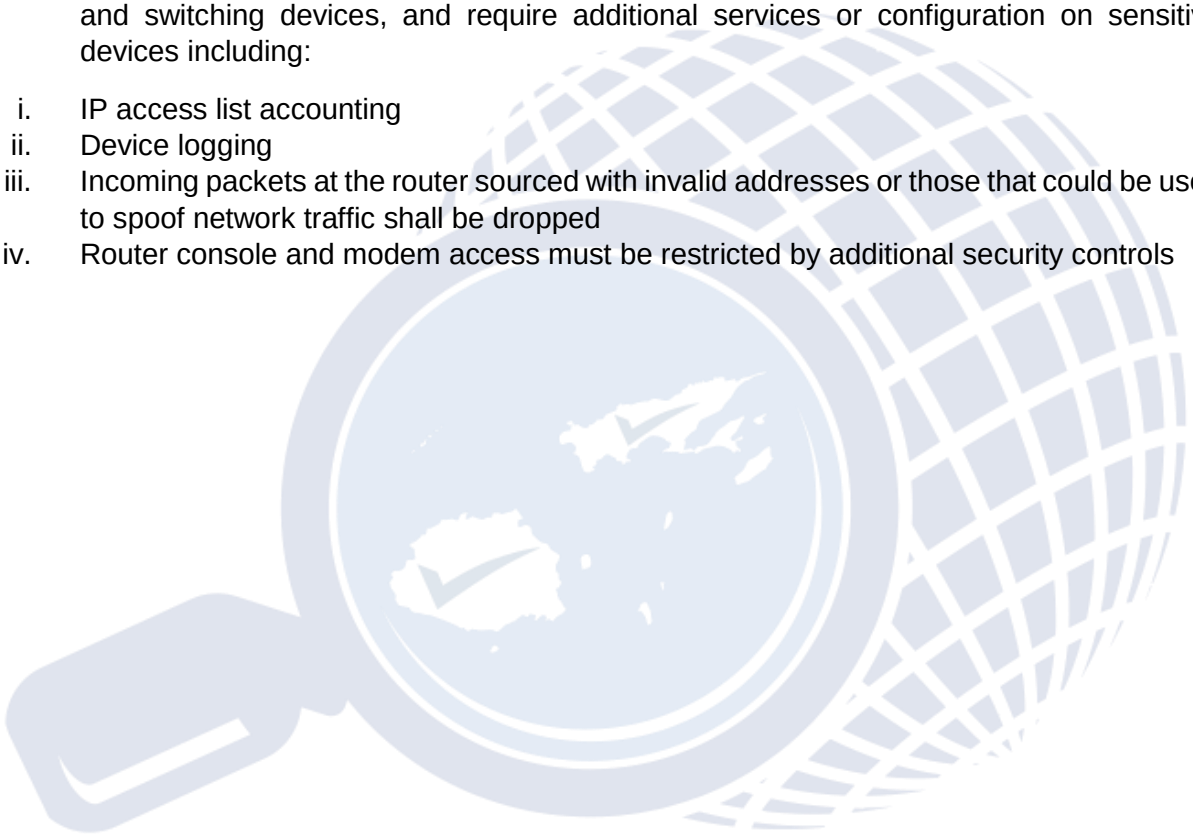
"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

l) Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path.

m) Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

n) The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

i. IP access list accounting
ii. Device logging
iii. Incoming packets at the router sourced with invalid addresses or those that could be used to spoof network traffic shall be dropped
iv. Router console and modem access must be restricted by additional security controls



ANNEXURE 19 – Wireless Communication Standard

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to OAG network.

Purpose

To specify the technical requirements that wireless infrastructure devices must satisfy to connect to the OAG network.

Policy

19.1 General Requirements

All wireless infrastructure devices that connect to the OAG network or provide access to OAG information must:

a) Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

b) Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

c) All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

19.2 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to the OAG network, such as those behind Enterprise Teleworker (ECT) or hardware Virtual Private Network, must adhere to the following:

a) Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS

b) When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

c) Disable broadcast of Service Set Identifier (SSID)

d) Change the default SSID name

e) Change the default login and password

ANNEXURE 20 – Wireless Communication Policy

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to OAG network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the IT Unit are approved for connectivity to the OAG network.

Purpose

To set the standard for network operation and security, specifically in the context of wireless network access. The configuration, installation, and maintenance of wireless communication network access point devices, if unmanaged, could result in severe interference with other network users and serious security risks.

Policy

a) Use OAG configured authentication protocols, username and password for connecting to wireless infrastructure.

b) Wireless infrastructure devices that provide direct access to OAG network must:

   i. Enable Wi-Fi Protected Access Enterprise (WPA2.Enterprise) protocol. It also must use Advanced Encryption Standard (AES) with minimum of 128-bit key length.

   ii. Be configured to change the default SSID name.

   iii. Be configured with password protected SSID.

   iv. Be configured with firewall feature sets on the Wi-Fi controller to protect inter user communication and OAG IT assets.

c) OAG guests shall be provided with username and password to gain access to network.

General Requirements

All wireless infrastructure devices that reside at the OAG site and connect to the OAG network, or provide access to information classified as OAG Confidential, or above must:

a) Abide by the standards specified in the Wireless Communication Standard. (Refer to Annexure 19

b) Be installed, supported, and maintained by an approved support team.

c) Use OAG approved authentication protocols and infrastructure.

d) Use OAG approved encryption protocols.

e) Maintain a hardware address (MAC address) that can be registered and tracked.

f) Not interfere with wireless access deployments maintained by other support organizations.

Home Wireless Device Requirements

a) Wireless infrastructure devices that provide direct access to the OAG network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard. (Refer to Annexure 19)

b) Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the OAG network. Access to the OAG network through this device must use standard remote access authentication.

ANNEXURE 21 – CONFIDENTIALITY AGREEMENT

CONFIDENTIALITY AGREEMENT

This Agreement is made this day of , 2020.

BETWEEN : THE OFFICE OF THE AUDITOR GENERAL (OAG) of 6-8th Floor, Ratu Sukuna House, Suva

AND : [INSERT NAME] <registered address> ('the Recipient Party')

RECITALS:

A. OAG is <*insert mission statement etc*>.

B. The Recipient Party has been engaged or is proposed to be engaged for <*insert relevant engagement etc*>.

C. In due consideration of the works to be carried out, OAG shall only engage the Recipient Party for works on the proviso that the Recipient Party enters into this Confidentiality Agreement with OAG, regardless of whether any works is carried out by the Recipient Party.

WHEREAS THE PARTIES HEREBY AGREE AS FOLLOWS:

1.0 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless the context otherwise requires:

(a) "**Confidential Information**" shall mean and refer to any information, including, but not limited to, trade secrets, business processes, business concepts, business plans, business proposals, techniques, data of any kind, proprietary business information of any sort, drawings/ schematics, research or development projects and their results, tests, or any non-public information which concerns the business of OAG and/or the Recipient Party, its operations, ideas or plans of a party to this agreement conveyed to any other party by any format or means, including, but not limited to, written, typed, magnetic, verbally or through any other medium whatsoever;

(b) The "**Recipient Party**" shall mean a party to this agreement that receives or is entitled to receive **Confidential Information** or any other party to this agreement;

(c) The "**Disclosing Party**" shall mean a party to this agreement that disclosed (or discloses **Confidential Information**) to other parties to this agreement.

1.2 In the interpretation of this Agreement:
(a) clause headings will be disregarded;
(b) words importing the singular include the plural and vice-versa; and
(c) words importing a gender include the other genders.

2.0 CONFIDENTIALITY

2.1 This Agreement is not applicable to information that is:
(a) Available to the public through no wrongful act of the receiving party;
(b) Available through OAG's public-relations mechanisms (i.e. through press releases, marketing brochures, website content);
(c) Information that has been published for the purposes of public dissemination;

2.2 Confidentiality imposed under this agreement is for an indefinite period unless stated otherwise by OAG in writing.

2.3 The recipient of "**Confidential Information**" shall not disclose or communicate any "**Confidential Information**" to any other person or party/parties or entities for any purpose or reason without the written consent of OAG.

2.4 Where the recipient party is an organization or entity rather than an individual, the recipient organization may disclose "**Confidential Information**" **only** to its management and employees within its organization who have been advised of the terms of this agreement and who have a need to know such "**Confidential Information**"..

2.5 Should the "**Recipient Party**" wish to disclose "**Confidential Information**" to outside parties such as consulting lawyers, accountants, engineers and others, the Recipient Party must first obtain prior written consent from OAG.

2.6 The "**Recipient Party**" shall **not** make copies of, nor otherwise duplicate in any manner, the "**Confidential Information**" covered by this agreement without first obtaining prior written consent from OAG.

3.0 DISCLOSURE OF CONFIDENTIAL INFORMATION

3.1 The Recipient Party shall not, under any circumstances disclose any "**Confidential Information**" to any party/parties external to this agreement except in accordance with the terms of this Agreement.

4.0 RETURN OF CONFIDENTIAL INFORMATION

4.1 Upon receipt of written notification from OAG, the Recipient Party shall promptly return ALL Confidential Information to OAG (including any copies of any such Confidential Information should OAG have authorised the making of copies).

5.0 INTELLECTUAL PROPERTY

5.1 The parties entering this agreement hereby stipulate that all title and ownership of or relating to any intellectual property, including but not limited to, concepts/ideas, creations, documents, contracts, improvements or any other property subject to copyright protection or intellectual property rights as developed or resulting from work carried out under this agreement, either directly or indirectly shall vest solely with OAG.

5.2 Any rights to jointly develop intellectual property shall be set forth once again by OAG, if applicable in a separate agreement document.

5.3 The Recipient Party is prohibited from making use of or copying any document, contract and/or proposal in which OAG owns copyright by virtue of this Agreement.

6.0 FURTHER ASSURANCES

6.1 The parties will do everything reasonably necessary to give effect to this Agreement and to the transactions contemplated by it and will use all reasonable endeavours to cause relevant third parties to do likewise.

7.0 CONTINUING OBLIGATIONS AND INDEMNITY

7.1 Clauses in this Agreement survive expiration or termination of any works carried out by the Recipient Party after entering into this Agreement and they will remain in full force and effect and binding on the Recipient Party concerned.

8.0 SUCCESSORS AND ASSIGNEES

8.1 This Agreement will be binding on and continue for the benefit of each party, its successors and permitted assignees survive termination of this Agreement.

9.0 VARIATION

9.1 No variation of this Agreement will be binding on the parties unless in writing and signed by all parties.

10.0 REMEDIES

10.1The parties hereby recognise and agree that irreparable damage and harm will result to OAG in the breach of this agreement by any party to this agreement and that damages will not be an adequate remedy. Therefore, OAG may, without prejudice to any other legal rights at its disposal, obtain injunctive relief to prevent any or further breaches of this Agreement.

10.2 The violating party/ parties agree that it/ they shall indemnify OAG for all the costs and damages incurred as a result of the breach of this Agreement.

11.0 APPLICABLE LAW AND JURISDICTION

11.1 Law

This Agreement is governed by and is to be construed in accordance with the laws of Fiji.

11.2 Jurisdiction

The parties submit to the non-exclusive jurisdiction of the courts of Fiji in respect of all matters arising out of this Agreement.

12.0 COUNTERPARTS

12.1 This Agreement may be signed in any number of counterparts and all such counterparts taken together are deemed to constitute one and the same document.

13.0 ENTIRE AGREEMENT

13.1 This Agreement constitutes the entire agreement and the basis of the transaction between the parties in relation to its subject matter and it supersedes all other communications, negotiations, arrangements and agreements between the parties whether oral or in writing.

IN WITNESS WHEREOF the parties state that they have read and accepted all the terms and conditions stipulated in the present Agreement.

Signed at:_____, this _____ day of _____, 20_____.

For the OAG:

_____
Auditor General or Deputy Auditor General

For the Recipient Party:

_____
<Insert Name>

In the Presence of:

_____
Signature of Witness
Name of Witness

_____
Signature of Witness
Name of Witness

16 Review & Monitoring

A review and update of this policy will take place on an annual basis or when changes requiring amending the Policy to ensure that the policy remain relevant and updated.

Such modifications shall relate to changes in roles and responsibilities, release of new legislation or technical guidance or the identification of a new policy area.

The Executive Management Committee will approve all revisions to this Policy. When approved a new version will be issued, and users will be informed of the changes

17 Who to Contact About this Policy

Any queries is directed to Deputy Auditor-General

18 Approval

The Information Security Policy becomes effective on the date approved by the Executive Management Committee

19 Revision/Change Log

Version 1.0	
Policy endorsed by:	Executive Management Committee
Policy approved by:	Executive Management Committee
Policy effective from:	1 April 2020
Policy to be reviewed by:	31 March 2021
Manager responsible for policy:	Manager Corporate Services