المركز الإحصائي
لدول مجلس التعاون لدول الخليج العربية
GCC-STAT

Information Security Policies

Tuesday, April 5, 2016
Version: 1.1

Document Management Information

Item	Description			
Document Title:	Information Security Policies Manual			
Department:	Information Technology			
Doc Ref:	GCC-Stat-IT/ISMS-PLCY-INT/0001			
Version Number	1.0			
Classification	○ Public	◉ Internal	○ Confidential	○ Top Secret
Publish Date:				

Version Number	Date	Author(s)	Remark
1.0	June 3, 2014	Nalakha Kumarasinghe	

Version Number	Date	Reviewer(s)	Remark
1.0	June 12, 2014	Eng. Fahad M. Senan	

Version Number	Date	Approver(s)	Remark
1.0		Eng. Mubarak Al Suti Mr. Sabir Al Harbi ISSC	

Document Revision Record

Version	Date of Revision	Author/ Updated By	Reviewed By	Remarks/Reasons
1.0	June 3, 2014	Nalakha Kumarasinghe	Eng. Fahad M. Senan, Eng. Mubarak Al Sulti	Creation
1.0	June 12, 2014	Eng. Fahad M. Senan	Eng. Mubarak Al Sulti	Arabic Translation
1.1	April 05, 2016	Eng. Mubarak Al Sulti	Eng. Mubarak Al Sulti	Amendments

CONTENTS

INTRODUCTION

Information consists in many forms – stored / transmitted electronically or in a written / printed form or shared during spoken conversations. Information is a valuable asset for GCCSTAT and is essential for GCCSTAT to:

- Protect this valuable asset from unauthorized or accidental access and modification and;
- Ensure availability of this information to the right people at the right time.

This manual outlines the policy framework for establishing Information Security in GCCSTAT and discusses how GCCSTAT will manage, protect and distribute sensitive information. The policy manual is divided into two parts: High-Level Policies and Detailed Policies.

Part I: High-Level Policies. This part discusses policies at a higher level and contains three policies:

- *Information Security Policy*: This policy set by the senior management establishes the management direction, support and commitment for Information Security initiatives in GCCSTAT.
- *Acceptable Use Policy*: This policy defines acceptable practices relating to the use of GCCSTAT's Information resources, which includes but not limited to the computing equipment, software, network services, Email services, Internet services and storage media. This policy contains the minimum that every employee should know.
- *Security Awareness Policy*: This policy informs staff that security is everyone's responsibility and that everyone is required to learn about security and to attend events / trainings / workshops concerning security.

Part II: Detailed Policies: This part divides security policies into ~~eleven~~ main areas:

Data Ownership, Antiviral and Malicious Programs, Internet-related Policies, Access Control, Network Policies, Legacy and Web Applications, Physical Security, Operations Management, Business Continuity Policy and Personnel & Third Party, Security Incident Management and Audit, Compliance management policies. Each area is subdivided into additional policies addressing the various levels of information security.

All concerned parties must seek to apply this policy, and any breach of any of policy will be subject to disciplinary action proceedings.

PART I

INFORMATION SECURITY POLICY STATEMENT

Information Security Management System Policy

GCC-Stat is to secure its Statistical Information and Information Systems in a manner which complies with legislation and meets accepted best practice by protecting it from unauthorized use, disclosure or destruction. Technology and Information Department will ensure the continuity of its operations and mitigate organizational damage in the event of a security incident by implementing appropriate controls. All staff of GCC-Stat are responsible for establishing and improving procedure to implement Information security policies within their areas of responsibility.

Policy Objective:

GCC-Stat ISMS policy to ensure that;

- Prevent Information Security Risks to an acceptable level
- Protect all information from un authorization access
- Provide protected suitable physical security and environmental controls, and where appropriate
- Maintain employees' awareness of information security
- Classify all information according to its importance to protect it from modification or divulged to any third party without authorization
- Continually improve ISMS based on employee feedback, incidents, audit findings and technologies

Policy Scope:

This policy covers all forms of information and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, CD's or other available storage media, or spoken in conversation and over the telephone. This policy includes all employees (on permanent or temporary contracts and full and part timers), contractors, consultants, service providers, as well as the GCC-Stat's facilities, software, paper documents and all other documents through which GCC-Stat special information can be accessed. For detailed scope, please refer section 1.2

PART II

HIGH-LEVEL POLICIES

1. INFORMATION SECURITY POLICY

1.1. Purpose

The purpose of this policy is to:

1.1.1. Establish the management direction, support and commitment for Information Security initiatives in GCCSTAT.

1.1.2. Inform all GCCSTAT personnel, other government agencies, customers and business partners who have access to GCCSTAT information of their responsibilities and obligations with respect to Information Security.

1.1.3. Ensure that adequate resources are applied to implement an effective Information Security Management System.

1.1.4. Identify and Minimize risks and the extent of loss or damage from a security breach or exposure to GCCSTAT, the Government, customers and business partners.

1.1.5. Ensure the continuity of services to GCCSTAT's customers and business partners.

1.1.6. Identify and review security metrics on an ongoing basis to ensure the effectiveness of the Information Security measures.

1.2. Scope

This policy covers all forms of information and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, CD's or other available storage media, or spoken in conversation and over the telephone. The policy covers:

1.2.1. All Users of GCCSTAT information, including service providers of GCCSTAT.

1.2.2. Facilities: Includes all equipment, as well as the physical and environmental infrastructure:

- Computers of all sizes, whether general or special purpose, including Personal Computers. Peripherals, Workstation and Access Devices.
- Telecommunications and Data Communications cabling and equipment. Local and Wide Area Networks.
- Environmental control systems including air-conditioning and other cooling, alarms and safety equipment.
- Utility Services including electricity, gas and water.
- Buildings accommodating personnel and equipment.

1.2.3. Data: Includes both raw and processed data:

- Data files, regardless of their storage media including hard copies and data in transit
- Information derived from processed data regardless of the storage or presentation media.

1.2.4. Software: Includes locally developed programs and those acquired from external sources:

- Application Software, Operating System software and all associated utilities and support programs.
- Application enabling software including data base management, middleware, telecommunications and networking software.

1.2.5. Paper Documents: include systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.

1.2.6. Personnel: include employees, contractors, consultants, service providers, representatives of customers and other bodies that access GCCSTAT's information and data.

1.3. Policy

1.4.

1.3.1. GCCSTAT shall implement all relevant and all possible measures to achieve the following security objectives:

- Availability: Adequate controls / safeguards shall be in place to ensure accessibility of information and deliverability of services to authorized users, customers and business partners when required and ensure recoverability in the event of a disruption.
- Integrity: Adequate controls / safeguards shall be in place to ensure completeness and accuracy of Information during the capture, storage, processing and presentation of information and protect against unauthorized modification or destruction.
- Confidentiality: Adequate controls / safeguards shall be in place to ensure that information is being made available or disclosed to authorize processes, entities or individuals ONLY.
- Authenticity: Adequate controls / safeguards shall be in place to uniquely identify users of information assets to the information being accessed.
- Accountability: Adequate controls / safeguards shall be in place to ensure responsibility for information and actions undertaken by providers and users of information.

1.3.2. Information assets owned, leased or rented by GCCSTAT shall be solely for the conduct of GCCSTAT business; no private use, or use for any other purpose shall not be permitted

1.3.3. All of GCC-STAT's critical assets (e.g. hardware, software, equipment and data) should be identified and appropriately protected. A formal inventory of all assets should be compiled. All Assets and Information should be appropriately classified and labelled as per the business's requirements.

1.3.4. Information security education, awareness and training shall be made available to GCC-STAT personnel.

1.3.5. This Information Security Policy and supporting Policies, Procedures and Guidelines not limited to Information Security will be made available online format through the Intranet System.

1.3.6. The Information Security policy, supporting policies, guidelines and procedures should be reviewed on a yearly basis.

1.3.7. Compliance with the Policy will be monitored on every 2 years. Security logs and audit trails will be produced to monitor the activities of users in their usage of information assets.

1.3.8. All access to GCCSTAT resources and information should be on a 'Need to Know' basis. Resource rights which are not explicitly assigned should be assumed to be denied.

1.3.9. The Chief Information Security Officer (CISO) will be responsible in co-ordinating and the implementation of all security policies and related security initiatives and tasks. An "Information Security Forum" and / or an Information Security Steering Committee" maybe created as appropriate.

1.3.10. The Chief Information Security Officer (CISO) will ensure that security issues are addressed and will devise a mechanism to prevent recurrence in the future.

1.3.11. Encrypt information classified as "Confidential" and "Highly confidential" while being transmitted outside GCC-STAT through the network or stored in the database or in other storage media.

1.3.12. The software developed for or used in GCC-STAT should undergo a proper security approval prior to moving to the production environment.

1.3.13. GCCSTAT reserves the right to monitor information traffic and all communication regardless of the medium being used, taking into consideration to obtain the General Director's approval with regard to the medium used and that it does not conflict with privacy protection laws and regulations.

1.3.14. The perimeter network of the GCC-Stat must be protected using appropriate hardware and software and monitored on an annual basis, taking into account the need to obtain the General Director's approval with regard to the medium used and that it does not conflict with privacy protection laws and regulations.

1.3.15. To provide protection against common threats to GCC-STAT, appropriate safeguards should be in place, including anti-virus programs, firewalls, Intrusion Prevention Systems (IPS) and other technology requirements.

1.3.16. Regular checks on network, servers and other equipment should be conducted in order to make sure that the network is secure
1.3.17. Proper and detailed procedures should be developed for implementing security.
1.3.18. All sensitive logs should be written on read-only discs to avoid alteration attempts. Only authorized persons should review the logs.
1.3.19. All documentation in the GCC-STAT should have a version control page with the document's history. All pages should be numbered.
1.3.20. All security incidents, weaknesses and breaches of information security, actual or suspected shall be reported to, and investigated by the relevant authorities not limited to Systems Administration and Incident Response.
1.3.21. Disciplinary action, according to the career system in force in GCC-STAT maybe taken.
1.3.22. The Computer Incident Response Team should have a documented Computer Emergency Response Plan which includes all necessary procedures.
1.3.23. Proper checking for vulnerability of all systems should be carried out on a regular basis (every 2 years) with the help of a Penetration Test.
1.3.24. Physical security is of prime importance. All efforts should be made to secure the physical perimeter, physical entry points, office rooms and delivery/loading areas.
1.3.25. Proper measures should be taken for securing all equipment, power supplies and cables.
1.3.26. Security of equipment while being maintained off-premises should be assured.
1.3.27. All employees and contractors should wear their identity badges and ensure it is visible when on the GCCSTAT premises.
1.3.28. Discussion of sensitive information in public places such as elevators or cafés is strictly prohibited.
1.3.29. All advertisements for jobs and help should be reviewed thoroughly and should not disclose any sensitive information.
1.3.30. If an GCCSTAT employee is presenting a paper, giving a presentation or delivering a speech in a public forum or conference, all material must be reviewed by his/her immediate manager prior to presentation.
1.3.31. An annual Information Security Audit should be performed to check the effectiveness of implemented controls. The Director of Information Security System shall review the report of the audit and then submit to the management and appropriate measures taken to enhance security within GCC-STAT on yearly basis.
1.3.32. A proper Business Impact Analysis and Risk Assessment should be performed for all critical business systems, either by the Director of Technology and Information in cooperation with Chief Information Security Officer and Risk Officer or by an outsourced resource as appropriate.

1.3.33. GCC-STAT employees should comply with all the legal requirements as specified by the stat members. Employees shall not indulge in an activity that is illegal under the local or international law.

1.3.34. All concerned should ensure compliance to this policy, the other policies included in the manual and related standards, procedures and guidelines (outside this manual).

Information Security Steering Committee

1.3.35. An Information Security Steering Committee (ISSC) with management leadership is established to approve the Information Security Policy, assign security roles and coordinate the implementation of security in GCC-STAT.

1.3.36. The objective of ISSC is to ensure that there is clear direction and visible management support for information security initiatives. The committee would also review and monitor the significant development in information security related projects, incidents handling and risk mitigation.

1.3.37. The permanent members of the ISSC shall comprise of the following:

Director General of the centre or whoever is authorized by the statistical department directors, provided that the Director of Technology and Information, Information Security Expert.

Information Security Co-ordination and Review

1.3.38. Chief Information Security Officer (CISO) coordinates the security initiatives taken by all Departments and communicates all feedback/requirements to modify the existing security infrastructure for effective deployment of security policies and procedures. The ISSC reviews the reports submitted by Chief Information Security Officer.

1.3.39. A risk assessment and mitigation exercise shall be done once a year in line with the methodology followed. The risk mitigation strategy shall be approved by the top senior management.

1.3.40. ISSC shall plan and conduct audit of the Information Security Management System (ISMS). These audits shall be carried out by an internally formed audit team or external consultants. ISSC shall decide the frequency of audits to suit its operations.

1.3.41. Segregation of duties for every employee shall be defined in order to prevent misuse of information or services.

1.3.42. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed. Proper contract / service level agreements shall be in place with the vendor with proper security requirements. For business critical services, specify a penalty clause in the agreement with the vendor for delay in service.

1.4. Approach

Information Security Management System (ISMS) is a systematic approach to manage information so that it remains secure. GCC-STAT shall adopt suitable international standards and best practices to implement an ISMS. The ISMS shall include all of the policies, procedures, plans, processes, practices, roles, responsibilities, structures, resources (Hardware and Software), that are used to protect and preserve information. As a part of the ISMS, risk management techniques and processes shall be continuously employed to:

- Identify and determine the value of Information Assets to GCC-STAT and;
- Implement appropriate protection measures based on the identified value and associated risks.
- The risk management process shall take into consideration the relevant legal and statutory compliance requirements.

1.5. Responsibility

1.5.1. The Chief Information Security Officer is responsible for Information Security, shall co-ordinate the development of guidelines and procedures for the implementation of this policy, and he will be responsible for an on-going review of their effectiveness, and he must ensure that personnel are fully informed of their obligations and responsibilities with respect to these guidelines and procedures.

1.5.2. All personnel, whether employees, contractors, consultants or visitors, are required to comply with the information security policies, guidelines, procedures and mechanisms and to play an active role in protecting the information assets of GCCSTAT. They must not access or operate these assets without authority and must report security breaches or exposures coming to their attention to the Director of Technology and Information.

1.5.3. The directors of the statistical departments, as members of the Steering Committee of information security, have a responsibility as custodians of the data and other information assets that support the business activities performed under their supervision to ensure that those assets are adequately secured. They must also ensure that the appropriate information security guidelines, procedures and mechanisms are observed in the performance of these activities.

1.5.4. The Director of Technology and Information is responsible for the day-to-day administration of the information security procedures and practices. The Chief Information Security Officer reports directly to the Director of Technology and Information on the performance of the information security procedures and practices.

2. ACCEPTABLE USAGE POLICY

2.1. Purpose

The purpose of the Acceptable Use Policy is to communicate the acceptable behaviour of the employee which is necessary to ensure security of the systems, assets and information.

2.2. Scope

The scope of this policy covers all permanent/contract employees, consultants and vendor/third parties' assigned persons working for GCC-STAT.

The policy also applies to all IT equipment/services owned or rented by GCC-STAT.

2.3. Policy

2.3.1. Security is everyone's responsibility every day. All employees of GCC-STAT should follow the security policies applicable to their area.

2.3.2. GCCSTAT resources (including but not limited to Email and Internet) are meant for business use and should be used for business purposes only.

2.3.3. Technology and Information Department through the information security expert, will be issuing guidelines though intranet or email that need to be followed.

2.3.4. An excuse of unawareness of a security policy will not be acceptable.

2.3.5. All of the information stored on or transmitted over GCC-STAT's resources remains GCC-STAT's property and GCC-STAT has the right to monitor and audit them, taking into the principles and controls of privacy.

2.3.6. All of GCC-STAT's confidential information should be treated in strict confidence. Copying or transmitting of the information is strictly prohibited except when required for GCC-STAT business.

2.3.7. It is the employee's responsibility to protect all of the passwords and pass phrases assigned to them. They should not share these with any other person.

2.3.8. A password should be changed as per the password policy.

2.3.9. All desktop computers and laptops must have a password-protected screensaver which should activate after a period of no longer than 10 minutes of non-usage.

2.3.10. All sensitive information stored in a laptop should be password protected.

2.3.11. All computers and related devices should run the latest antiviral software. No employee is allowed to disable or deactivate the virus detection engine.

2.3.12. The e-mail and Internet policies should be followed while using e-mail or the Internet.

2.3.13. No unauthorized copying of software is allowed.

2.3.14. No GCC-STAT resources should be used to test software as it may malfunction or be malicious in nature. An exception is made for software that is to be used in GCC-STAT, as they have their special testing environment that is not associated with the production environment.

2.3.15. No person is allowed to browse the GCC-STAT network from his PC or any other resource.

2.3.16. Probing and port scanning of external and internal servers is strictly prohibited unless it is part of the official penetration test undertaken by GCC-STAT and appropriate counter measures are taken.

2.3.17. No vulnerability probing or similar software should reside on any computer except when being used by the Systems Administrator for the purposes of assessment. As soon as the assessment has been completed, all such software should be removed from the system.

2.3.18. No games should be stored or played on GCC-STAT computers without management approvals.

2.3.19. Operating systems must be updated.

2.3.20. Computers desktops must be secured.

2.4. **Responsibility:** All GCC-STAT Employees.

3. SECURITY AWARENESS POLICY

3.1. Purpose

The purpose of this policy is to keep employees up to date with information security which is changing at an astonishing pace.

3.2. Scope

The policy applies to all employees, irrespective of the positions being held.

3.3. Policy

3.3.1. The Director of Technology and Information under the supervision of the information security expert will organize at least one workshop per year and the attendance of every employee will be mandatory, and new staff must be informed about management policies.

3.3.2. In the case where an employee has not attended the workshop, his/her respective manager will be informed to take proper action or reschedule an alternative workshop.

3.3.3. If necessary, the Director of Technology and Information takes help of brochures, Posters and/or special Security Awareness Screen Saver to increase the Information Security.

3.3.4. A Security Awareness Booklet and Brochure will be given by HR Department to every new employee. The last page will be the “End User Information Security Policy Undertaking” that needs to be signed by the employee.

3.3.5. It is the responsibility of every individual to keep him/herself up to date through involvement in security trainings conducted by GCC-STAT.

3.3.6. Any security breach or query about security should be communicated to Director of Technology and Information immediately.

3.3.7. Knowledge of security policies is one of the areas that will be emphasized to all GCCSTAT employees.

3.4. Responsibility

- Information Security Expert responsible to arrange for the awareness workshop.

PART III

DETAILED POLICIES

4. GENERAL INFORMATION SECURITY CONTROLS POLICY

4.1. Purpose

The purpose of this policy is to provide GCC-STAT's management direction and support for Information Security in accordance with business requirements and relevant laws and regulations.

4.2. Scope

This policy applies to GCC-STAT's all Information assets, permanent and contract employees, the third party vendors, business partners, Contractors dealing with GCC-STAT

4.3. Policy

4.3.1. All employees/non-employees accessing GCC-STAT classified information has a role to play in the protection of the information.

4.3.2. All new information processing facilities shall be set up in accordance with the Information Security Policy of GCCSTAT and if required, will undergo a review by the ISSC / IGB.

4.3.3. Based on requirements, specialist advice (in-house or outsourced) shall be sought for all decisions related to information security.

4.3.4. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

4.4. Responsibility

All Department Directors, Employees, Information Security Officer

.

5. DATA PROTECTION AND CLASSIFICATION POLICY

5.1. Purpose

The purpose of the policy is to implement proper data ownership for Information Security. The owner of the data needs to be clearly specified with corresponding duties and responsibilities, including (data classification, data access and data dissemination as per the data dissemination policy).

5.2. Scope

The policy applies to all employees who at any time are responsible for data handling, using and owning.

5.3. Policy

5.3.1. The Data Owner should be specified for each application.

The Data Owners:

- Director General's Office.
- Deputies of Director General and Directors of Statistics Departments.
- Director of Legal Department.
- Director of Finance and HR Department.

The Data Custodian facilitate the storage of all information:

- Director of Technology and Information Department.

5.3.2. The Data Owner will communicate the importance of the data, level of sensitivity, controls and monitoring requirements to the Data Custodian.

5.3.3. The Data Custodian may not take any action on the data without the permission of the Data Owner.

5.3.4. It is the responsibility of the Data Custodian to ensure that data is backed up and stored at a secure place.

5.3.5. The Data Custodian will make sure that there are proper safeguards in place to recover from any Disaster.

5.3.6. Any data that is not on the server or is not been backed up by the GCC-STAT backup facility will be the responsibility of the data owner to make sure that recovery is possible in the case of system failure or hard disk crash.

5.3.7. The Data Custodian will make sure that all adequate controls are in place, as specified by the Data Owner.

5.3.8. The Data Custodian should maintain proper documentation of all activities involving the Owner's data.

5.3.9. The Data Custodian will inform the Data Owner of any risk or shortcomings as soon as they are identified.

Data Ownership Classification:

5.3.10. The following table identifies the types of data, data usage and accessibility, and determines the level of security in the Centre. All information, in electronic and hard copy form, would carry a classification. Any information that does not carry a marking would be default considered as "internal".

Classification	Definition	Examples
Public	Applies to Information which has been approved by the executive management for release to the public	Brochures Press release GCCSTAT website Countries statistical data Raw data and data for dissemination General geographical maps of countries
Internal	Information that is generally available to all employees.	Internal telephone directories Organizational charts Media and News Services Request Forms
Confidential	Information is distributed on a *need-to-know* basis	Financial information Policies in draft Network Diagram Non-Disclosure Agreements, Service level Agreements Administrative decisions Private Contracts
Top Secret	Information that contains high-level business or technical information which discloses GCC-STAT's strategic activities Information that contains an employee's personal information, benefits and/or confidential financial status.	GCC-Stat long-range business plans IT strategies Financial results prior to public release Salary information

Amendment of data ownership and privacy

5.3.11. Any modification in the proprietary markings for 'Internal and Confidential' information shall be done in concurrence with the Directors. For modification to 'Top Secret' markings Director General or ISSC's approval is required

Storage and Access to Confidential Information

5.3.12. The table below provides guidelines for accessing and storing information that bears one of the following proprietary markings:

Classification	Authorised Access	Storage Requirements
Public	Available for everyone without permission.	No controls required to protect confidentiality of public data. Some level of control is required to prevent unauthorized modification or destruction of Public data.
Internal	GCC-STAT employees for conducting GCC-STAT's business operations. Non-employees must be limited to those bound by a non-disclosure agreement.	Locking not required if access to the facility is limited to authorized employees or those bound by a nondisclosure agreement. Must be locked if unescorted access is allowed for non-employees not bound by a nondisclosure agreement.
Confidential	Identified authorized persons with a validated "need to know". Persons with an established and validated business reason for having access to the document. Non-employees bound by a nondisclosure agreement related specifically to the material	Must not be left unattended and must be locked when not in use.
Top Secret	Disclosed only to specific authorized persons and Identified authorized persons with a validated "need to know."	Must not be left unattended and must be locked when not in use.

Electronic Media Storage

5.3.13. Removable media like DVD, USB, PDA, Memory cards etc shall be used based on official purpose with proper justification in a valid request form with written authorization. Validity period for each request shall be limited only to three months from the date of access approval. Chief Information Security Officer shall remove user access to USB, DVD, PDA, and Memory Cards through a manual review.

Loss or Theft of Proprietary Information

5.3.14. When proprietary information has been compromised, lost, stolen, the security incident shall be reported immediately.

5.3.15. Sensitive marked documents shall be disposed off by either crosscut shredding. The owner of the proprietary information shall ensure that distribution recipients know and understand the proper disposal techniques.

5.3.16. Where GCCSTAT Proprietary, Confidential and Top Secret information is stored on any storage media (diskettes, hard disk drives, magnetic tape, CD-ROM etc.) the files must be completely erased or the media physically destroyed in a manner that renders the data unrecoverable.

Information Leakage

5.3.17. Opportunities for unauthorized disclosure, access and leakage shall be prevented. In order to achieve this, the following shall be considered:

- Outgoing information and communication shall be scanned.

- Regular monitoring of employees' system activities related to various ways of handling data like, copying, transmitting, printing etc.

Information Asset Identification and Classification (AIC)

5.3.18. Each Director shall own and maintain a list of all the information assets pertains to their Departments

5.3.19. All information assets shall be classified as per Confidentiality, Integrity and Availability by the respective asset owners. Each department may have a further distinct classification for the purpose of their understanding, show the classification to the information security steering committee for review and approval.

5.3.20. The inventory of information assets shall have the following details:

- Asset ID
- Type of Asset
- Asset Description
- Classification (CIA)
- Location
- Owner
- Serial Number
- Manufacture details
- Remarks

Security of System Documentation

5.3.21. Sensitive documents for example operating procedures, user's manual and technical documentation related to critical systems shall be adequately protected against unauthorized access and stored in a secured manner.

Intellectual Property Rights

5.3.22. Adequate procedures must be developed and maintained to ensure that compliance with legislative, regulatory and contractual requirements on the use the material in a fashion of which there may be intellectual property rights and on the use of proprietary software products. Intellectual property developed by any staff for use in GCC-STAT belongs to GCC-STAT.

Safeguarding Organizational Records

5.3.23. Critical and organizational records including personal information must be protected from unauthorized access, loss, destruction, theft, alteration, falsification, etc in compliance with statutory, regulatory, contractual and business requirements.

5.4. Responsibility

Data Owner, Data Custodian.

6. INFORMATION SAFEGUARDING POLICY

6.1. Purpose

This policy specifies the control and proper safeguard of information generated, stored and transmitted in GCC-STAT.

6.2. Scope

The policy applies to all forms of information regardless of what medium is used for their storage and communication.

6.3. Policy

6.3.1. The backup frequency and retention should be defined and implemented by coordination of data owner, Director of Technology and Information and Information Security Officer.

6.3.2. All backup should be verified to ensure that it is restorable.

6.3.3. Off-site backup of data and applications on critical machines is highly recommended, and should be carried out at least fortnightly.

6.3.4. CD-ROMs/DVDs or Tapes or External Hard disk should be used for the backup of configuration and other files.

6.3.5. The Data Owner should specify the data retention period.

6.3.6. No pirated or other illegal software may be used in GCC-STAT.

6.3.7. Any software bought from outside vendors or contractors should be installed only after proper permission from the Director of Technology and Information has been obtained.

6.3.8. The Application Program and data should be separated for security purposes.

6.3.9. All software should be tested in the test environment prior to being moved to the production environment.

6.3.10. Proper measures such as the installation of anti-virus software, firewalls, IDS and others should be taken to address external and internal threats.

6.4. Responsibility

All employees, Departments Managers and Information Security Officer.

ANTI-VIRUS AND MALICIOUS PROGRAM POLICY

7. ANTIVIRUS POLICY

7.1. Purpose

This document specifies GCC-STAT's policy related to malicious programs i.e. Viruses, Worms, Trojans and others.

7.2. Scope

The scope of the policy includes all electronic communication mediums as well as all storage media which can be infected or can store or propagate malicious programs.

7.3. Policy

7.3.1. All computers and devices should run the latest anti-virus software definitions as Approved and recommended by GCC-STAT Technology and Information Department.

7.3.2. E-mail with attachments coming from suspicious or unknown sources with signs of viruses should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail which he/she thinks may contain virus.

7.3.3. All removable media (e.g. CDs, flash and others) should be scanned for viruses before being used.

7.3.4. In the case of a virus being found, the Information Security Officer should be informed immediately. The Information Security Officer will investigate and take proper measures to avoid the event in future.

7.3.5. The e-mail Server should have the antiviral program installed and must check all of the e-mail attachments before sending it to individual mailbox.

7.3.6. All of the updates to the antiviral program should be automatic from the web or from a central server.

7.3.7. The Antivirus program should be supplemented by following components:

- Personal Firewall
- Antispyware and related safeguards

7.4. Responsibility

All employees, Director of Technology and Information and Information Security Officer.

8. INTERNET USAGE POLICY

8.1. Purpose

This document specifies GCC-STAT policy related to Internet Usage.

8.2. Scope

The scope of the policy includes all employees accessing internet, irrespective of their position.

8.3. Policy

8.3.1. Only official Internet connections should be used. No person is allowed to connect to the Internet through any other method other than the GCC-STAT network, as this would open an unsecured backdoor to GCC-STAT.

8.3.2. Internet facilities will be provided to only those employees who need them for business use. No Internet usage for personal purposes is allowed with the exception of research and educational matters for business needs.

8.3.3. While using the Internet, no person is allowed to abuse, defame, stalk, harass or threaten any other person, or violate local or international legal rights.

8.3.4. No person is allowed to upload, post, publish or distribute any inappropriate, indecent, obscene, profane, infringing, defamatory or unlawful information or material on the Internet while using the GCCSTAT resources.

8.3.5. No person is allowed to post personal advertisements or offer any goods or services using GCC-STAT's resources.

8.3.6. A visit to any obscene or socially unacceptable sites or sites which are non-business related will be considered a serious offence.

8.3.7. No one is allowed to use the chat services such as MSN, Yahoo, gTalk, Facebook, ICQ or any internet messenger. If any of these are to be used to communicate with a foreign consultant for problem solving or discussion purposes, prior permission from the relevant Department Manager and Director of Technology and Information is required.

8.3.8. Visitors or Guests accessing GCCSTAT's operational network through their personal laptops or smartphones is strictly prohibited. On request, they can connect their personal laptops or devices on GCCS-TAT's guest network,

8.4. **Responsibility:** All employees have internet access, Director of Technology and Information and Information Security Officer.

9. E-MAIL USAGE POLICY

9.1. Purpose

This document specifies GCCS-TAT policy related to e-mail usage (internal and external), including the receiving, replying, forwarding and auto reply functions.

9.2. Scope

The scope of the policy includes all permanent and contract employee irrespective of their position in GCC-STAT.

9.3. Policy

9.3.1. The e-mail facility is for business use only. The e-mail address allocated to an employee should not be used for personal purposes.

9.3.2. No free or public e-mail facility should be used to receive or send business-related information.

9.3.3. No non-business-related newsgroup may be added to your GCC-STAT e-mail address book.

9.3.4. The e-mail facility of GCC-STAT should not be used to spam others users, whether inside or outside GCC-STAT.

9.3.5. No harassing or insulting messages should be sent inside or outside of GCC-STAT.

9.3.6. No person is allowed to forward chain letters or pyramid schemes using the GCCSTAT e-mail.

9.3.7. No confidential document belonging to GCC-STAT may be sent to anyone, including to your own personal free-mail account.

9.3.8. If sensitive information needs to be sent to someone outside GCCSTAT, proper measures should be taken as specified by the Information Security Officer or Technology and Information Director.

9.3.9. GCC-STAT e-mail address should not be used when posting to newsgroups, as it may disclose GCCSTAT information. However, business-related newsgroups could be subscribed to using GCCSTAT e-mail address, provided permission is obtained from the respective manager.

9.3.10. The naming of e-mail address starts with the initial letter of the first name followed by the family of tribe name.

9.4. Responsibility:

All GCC-STAT employees.

Access Control Policies

10. LOGIN POLICY

10.1. Purpose

This document specifies GCC-STAT policy relating to login access to GCC-STAT information systems and computer resources and discusses in detail the related standards.

10.2. Scope

The scope of the policy includes all logins to applications and servers, irrespective of their operating platforms.

10.3. Policy

10.3.1. Every user should have a uniquely assigned login name and password to access GCC-STAT computer systems.

10.3.2. Each person is responsible for the login name & password assigned to him/her.

10.3.3. User login should be disabled after five unsuccessful attempts, and reactivated upon request to the Technology and Information Department.

10.3.4. A password should not be displayed in the screen.

10.3.5. In the case where an incorrect login name or password is entered, no response which reveals any information should be given. For example, systems should not respond with “Incorrect Password for xxx login name". This message will reveal that such a valid user name exists leaving the hacker having only to hack the password.

10.3.6. The login system should display the last login date and time. This will alert the user to any use of the system by an unauthorized person.

10.3.7. The system should log-off / lock out automatically after inactivity of fifteen minutes or a period specified by the Information Security Officer

10.3.8. In the case where a job function is based on a general USER ID, the USER ID should be changed to unique one.

10.3.9. Time-based access should be implemented for the user login, where possible.

10.3.10. In the case of a “Critical GCC-STAT Core System”, the end user should not be able to access the operating system command line.

10.3.11. For the issue of a new login name, a signed form indicating the relevant privileges is required, either in hardcopy or as part of the internal workflow software.

10.3.12. A login which is not successful should be logged and the logs should be reviewed at regular intervals.

10.3.13. A login ID not used for 90 days will be disabled automatically or with the request from the employee's Department Manager. Enabling such account will require a formal request from the department head.

10.3.14. In the case of an employee leaving GCC-STAT, the Department Director will be responsible for making sure that all the employee's system IDs are revoked or disabled prior to final settlement.

10.4. Responsibility

All employees, Systems Administrator and Information Security Officer.

11. PASSWORD PROTECTION POLICY

11.1. Purpose

This document specifies GCC-STAT policy related to password protection, change and maintenance.

11.2. Scope

The scope of the policy includes all employees, irrespective of their position.

11.3. Policy

11.3.1. All default passwords must be changed by the user prior to use of the system.

11.3.2. A password should not be less than 8 characters made up of a mixture of alphabetic, special and numeric characters, incorporating upper and lowercase letters.

11.3.3. A password should be changed every 45days or whenever compromised.

11.3.4. No common name or personal information should be used as a password e.g. dates of birth, spouse's name, pet name, employee number, resident number, mobile number or phone number or any other word that can be easily guessed.

11.3.5. A password should be different from the last 5 used passwords.

11.3.6. A password should always be kept secret and should never be disclosed to co-workers and colleagues.

11.3.7. No person should leave his/her PC or terminal without logging off or password protecting the screen.

11.3.8. Password should be stored in encrypted format and should never be in text format.

11.3.9. In case of emergency and unavailability of the Systems Administrator the password would be obtained from the person nominated by Information Security Officer.

11.4. Responsibility

All employees, Departmental Managers and the Information Security Officer.

NETWORK POLICIES

12. ROUTER AND FIREWALL SECURITY POLICY

12.1. Purpose

Routers and Firewalls are the most vulnerable components of perimeter security. This policy specifies the minimum security protection requirement for the perimeter routers and firewalls.

12.2. Scope

The scope of the policy covers the firewall and routers at the perimeter network. The policy is also applicable to devices such as proxy servers and ADSL routers.

12.3. Policy

12.3.1. Routers and firewalls should be placed in a physically secure area.

12.3.2. Local User Accounts should not be configured on the router. The firewall management terminal should be separate from the main box.

12.3.3. The password for routers should be encrypted using the "Enable Encryption" option.

12.3.4. Any service not explicitly allowed on firewall should be denied.

12.3.5. The Firewall computer should be a dedicated machine. It should not be used to run proxy, web or any other services.

12.3.6. Routers and firewalls should disallow all invalid IP addresses coming from the Internet i.e. 10.0.0.1 to 10.255.255.254 and 172.16.0.1 to 172.16.255.254, 192.168.0.1 to 192.168.255.254. with the exception of VPN connections.

12.3.7. Routers and firewalls should not allow IP broadcasts.

12.3.8. IP-directed broadcasts should not be allowed on the firewalls and routers.

12.3.9. Source routing should be disabled on the routers.

12.3.10. SNMP should not be enabled on either the firewalls or the routers. In cases where SNMP is needed for system management, a standardized SNMP community string should be used.

12.3.11. The firewall should be configured to stop (DDOS ATTACK).

12.3.12. Firewall should stop IP spoofing, fragmented packets and tear-drop.

12.3.13. The relevant Department Manager should approve the list of Access rules prior to deployment on routers.

12.3.14. Backup of the configuration files of the firewall and routers should be stored at a safe place.

12.3.15. The Audit log of the firewall should be regularly checked.

12.3.16. The firewall must hide all internal network addresses from the outside world.

12.3.17. A Firewall should filter the entire ActiveX and Java program.

12.3.18. Egress, i.e. the outgoing traffic should also be checked by the firewall.

12.3.19. Provided performance is not an issue, user level checking should be done at the firewall level, rather than at IP address level.

12.3.20. The Login Banner on the router should not display any welcome message. A warning message should rather appear:

"Warning: This is a Private Network. Any UNAUTHORIZED ACCESS TO THE SYSTEM IS STRICTLY PROHIBITED. If you are not authorized logoff now. All activities are logged. Any violator will be prosecuted."

12.4. Responsibility

Network Administrator, and Information Security Officer.

13. COMMUNICATION DEVICES AND CONNECTIONS SECURITY POLICY

13.1. Purpose

This document specifies GCC-STAT policy related to Dialup lines for computers and fax machines.

13.2. Scope

The scope of the policy includes all lines for the purpose of computer and fax connections.

13.3. Policy

13.3.1. No external dongles and hardware should be connected to any computer.

13.3.2. If there is any business need to use the dongle, prior permission is required from the Information Security Officer.

13.3.3. Fax machines should be used for business purposes only.

13.3.4. No analog phone line will be extended to an employee except for managers.

13.3.5. No faxes should be sent directly from a computer except for GCC-STAT fax server, where available.

13.3.6. Anything downloaded should be scanned for viruses prior to use.

13.4. Responsibility

All employees.

14. DMZ POLICY

14.1. Purpose

Demilitarized Zone (DMZ) is one of the most important zone of the GCC-STAT network. This policy defines the requirement for all equipment which is operated within GCC-STAT's DMZ, whether owned, leased, borrowed or brought by vendors for testing.

14.2. Scope

All DMZ equipment owned by GCC-STAT or outsourced.

14.3. Policy

14.3.1. Servers accessible from the Internet should be placed on DMZ.

14.3.2. There should be a defined owner for each DMZ equipment.

14.3.3. All equipment should be hardened to the maximum possible extent. There should be a System Hardening Checklist developed by the Systems Administrator for each DMZ component.

14.3.4. All required patches and fixes should be applied to all components of the DMZ and should be cross checked.

14.3.5. Only approved hardware, software and operating systems should be deployed in the DMZ.

14.3.6. All insecure services and protocols which are not needed, should be disabled.

14.3.7. If remote administration is required, a secured channel such as SSH or IPSEC should be used.

14.3.8. All security-related events should be logged.

14.3.9. In the case where a DNS is deployed, special care should be taken to protect the DNS server and to protect against DNS poisoning.

14.3.10. Proper auditing should be done at regular intervals; all logs of critical systems such as the Firewall.

14.3.11. Any new service should be approved by the Director of Technology and Information prior to being moved to the DMZ production environment.

14.3.12. All equipment belonging to outsourced companies, vendors or service providers must meet the GCC-STAT security criteria.

14.4. Responsibility

Network Administrator and Information Security Officer.

15. VIRTUAL PRIVATE NETWORK (VPN) POLICY

15.1. Purpose

The purpose of the VPN policy is to provide guidelines for secure remote access to the local networks.

15.2. Scope

The Virtual Private Network (VPN) policy applies to connections to GCC-STAT and to third parties including consultants, vendors and contractors.

15.3. Policy

As VPN is an extension of the GCC-STAT network, all of the security rules apply to the remote client as if they were within GCC-STAT.

15.3.1. All critical connections to the outside should use the safe channel. It is highly recommended to use IPSEC for VPN, where available.

15.3.2. It is highly recommended that a one-time password to be used where applicable.

15.3.3. "Tunnel Mode" is preferred whenever the VPN is used. If performance is an issue, "Transport Mode" may be used with the permission of the Information Security Officer.

15.3.4. All files transferred through VPNs should be subject to antivirus scanning.

15.3.5. The VPN timeout period is 15 minutes of inactivity.

15.4. Responsibility

Network Administrator and Information Security Officer.

16. WIRELESS COMMUNICATION POLICY

16.1. Purpose

The Purpose of the policy is to provide guidelines for network connections via wireless communication.

16.2. Scope

The policy covers all wireless devices such as mobile phones, PDA and laptop computers and others, which are connected to GCC-STAT network.

16.3. Policy

16.3.1. The Director of Technology and Information should approve all wireless devices connected to the GCCSTAT network.

16.3.2. A Strong Authentication server should be used to grant permission to the wireless devices.

16.3.3. Prior to the granting of a connection to the network devices, it would be preferable that the authentication server verify the hardware level address check (e.g. the MAC address) or in case of mobile phone the serial number.

16.3.4. Wi-Fi password should not be shared with anyone; it is associated with the user name and password.

16.3.5. Access to Wi-Fi connection will be provided on request with the approval of the department head and the Director of Technology and Information

16.4. Responsibility

Network Administrator and Information Security Officer.

17. REMOTE ACCESS POLICY

17.1. Purpose

This policy describes acceptable ways of connecting to the GCC-STAT network.

17.2. Scope

The scope of the policy covers all connections which are dialled-in or directly connected by GCC-STAT employees and or third parties, including consultants, vendors and contractors.

17.3. Policy

17.3.1. Remote Access should be used for the business purpose only, and must be encrypted.

17.3.2. A remote connection extends the GCC-STAT network, so all GCC-STAT policies apply to the remote connection.

17.3.3. An anti-virus check should be performed on all files downloaded through remote connections, and connection must be denied if the devices used does not conform to the GCC-Stat security standards.

17.3.4. All remote connections should be logged and monitored.

17.3.5. In case, Intrusion Detection System is deployed it should generate alert to the Systems Administrator, Information Security Officer if attack is detected.

17.3.6. Remote connection is not permitted until the explicit consent of the concerned department director is obtained, provided that this is justified by business requirements and carried out under the appropriate controls, in addition to signing the non-disclosure agreement.

17.3.7. All pc's connected to the remote connection system must be at least linked to a personal firewall and an anti-virus program, and these security controls must be activated all the time.

17.3.8. Users must not access the GCC-STAT's internal systems through public pc's such as: the computers available at internet cafes and the like, and they are not allowed to print any material through any public pc.

17.4. Responsibility

Network Administrator, Remote Connection Users and Director of Technology and Information

18. GENERAL APPLICATION DEVELOPMENT AND DEPLOYMENT POLICY

18.1. Purpose

This policy specifies the requirements for application development both in-house and outsourced by GCC-STAT.

18.2. Scope

This policy is applicable to all core business software and other software. However, it excludes the operating systems.

18.3. Policy

18.3.1. Formal security specifications are required for all systems developed in-house or outsourced.

18.3.2. No test account should be present on the production machine.

18.3.3. The production and development/test environments should be separate.

18.3.4. Any error in a system should be reported and must be traced to the programmer who developed the program.

18.3.5. Prior to the system being moved to production, proper documentation should be done.

18.3.6. No trial version, beta version or free software may be used in the production environment unless approved by management.

18.3.7. Proprietary business logic should reside on the central core server rather than on the desktop systems.

18.3.8. All computer programs, routines, applets and documentation should display the copyright statement.

18.3.9. After authentication, the username and password should not be recorded on the server.

18.3.10. All access should be on a “Need to Know” basis.

18.3.11. The application file storing the information should be password protected.

18.3.12. Either GCCS-TAT should own all of the core application Source Codes or there should be escrow agreements with the vendors who have provided the applications.

18.3.13. Prior to moving program to the production environment, there should be exhaustive testing of the application.

18.3.14. No application should be moved to the production environment without the proper signing of a UAT (User Acceptance Test).

18.3.15. The developer should not have any account on the production machine; prior to moving to the production environment all such accounts should be removed.

18.3.16. Databases should follow the password policy.

18.3.17. An update to the database should be carried out on a well-defined, secure channel.

18.3.18. In the case where a Data Warehouse application is used, access should be restricted to top and middle management.

18.4. Responsibility

Systems Analyst, Programmer and Director of Technology and Information.

19. WEB APPLICATION DEVELOPMENT POLICY

19.1. Purpose

This policy specifies the requirements for web application development in-house or out-sourced by GCC-STAT.

19.2. Scope

This policy is applicable to all web applications currently deployed, developed or would be developed in future.

19.3. Policy

19.3.1. A proper User ID and Password should be created for the Web Application User. Any Web Pages that communicate password and user name data should use the required protocol.

19.3.2. The Web Application password should not be displayed on the screen and the "Copy and Paste" feature on the password field should be disabled.

19.3.3. The Password should preferably be stored in a one way hash.

19.3.4. For Data that is of confidential nature, a secure channel should be used.

19.3.5. The 'Press back' button should clear the fields containing sensitive data.

19.3.6. An SSL connection should have an expiry time.

19.3.7. The Application should be programmed in such a way that in case of an error, there should be a standard error page rather than a system-generated error (e.g. 404) returned to the user as this would reveal the internal network.

19.3.8. The Web Server should not provide banner information.

19.3.9. The Directory listing of the CGI-BIN should not be accessible from the client.

19.3.10. The Input string from the customer should be validated prior to processing, as it may be manipulated to contain some secret command.

19.3.11. There should be an incident response procedure if something goes wrong on the server or if there is any security breach.

19.3.12. A Penetration test should be performed on the application as specified by the Information Security Officer.

19.4. Responsibilities

Director of Technology and Information, Systems Analyst, Web Admin, Web-Programmer and Information Security Officer.

20. GENERAL PHYSICAL SECURITY POLICY

20.1. Purpose

This policy specifies the requirements for physical security at GCC-STAT.

20.2. Scope

This policy is applicable to all physical areas of the offices of GCC-STAT, including those available now and those which may be added in the future.

20.3. Policy

20.3.1. The Director of Finance and Human Resource should define security zones within GCCSTAT. For example:

- Zone A: The reception area where anyone can walk in (Minimum Security).
- Zone B: Area accessible to employees and authorized visitors
- Zone C: Area to which only selected employees have access such as the Data Centre and other business-critical areas.

15.3.2. The Director of Finance and Hamman Resource should apply appropriate measures for each of the zones.

15.3.3. Office floor plans and diagrams of telephone, electrical, water and network cabling lines, as well as extinguisher locations should be documented and maintained.

15.3.4. A proper Access Control List with corresponding work times should be maintained.

15.3.5. The entrance of GCC-STAT should be properly guarded.

15.3.6. Proper fire prevention and detection mechanisms should be in place

15.3.7. A Telephone Directory for emergency phone numbers should be maintained and must be easily accessible.

15.3.8. A First Aid Box should be provided and must be easily accessible and regularly checked and replenished.

15.3.9. All areas of the office should be properly lighted.

20.4. Responsibilities

Finance and Human Resource Department, Network Administrator and Information Security Officer. In future, some of the tasks relating to physical security may be delegated to the Information Security Officer when that post is created. For the time being, the Finance and Human Resource Department will handle these tasks.

21. SERVER ROOM / DATA CENTER SECURITY POLICY

21.1. Purpose

This policy discusses the requirements for safeguarding the computer systems and personnel operating in the Server Room / Data Centre.

21.2. Scope

This policy is applicable to all physical areas of IT Department offices in GCCSTAT, including those which are available now and those which may be added in the future.

21.3. Policy

21.3.1. The data center must have a fire-resistant door that tolerates high temperatures resulting from fires, and for which eyes recognition or fingerprint systems must be used to open.

21.3.2. Access to the server room will be restricted to GCC-STAT authorized persons only.

21.3.3. No public visits or tours of the server room are allowed. Unless, approved by the Director of Technology and Information, Asst. DG or DG approval.

21.3.4. Vendor and third party representatives, if they visit the room, should be escorted.

21.3.5. A time-in and time-out register for Non-Administrative users should be maintained for the server room.

21.3.6. A proper fire alarm and fire extinguisher system should be in place.

21.3.7. Humidity control should be implemented and monitored.

21.3.8. A proper temperature should be maintained and monitored.

21.3.9. A proper Emergency procedure for the Server room should be developed and be easily accessible. Personnel should be trained so that the procedure is executed efficiently, when required. All procedures should be audited at regular intervals.

21.3.10. The Director of Technology and Information will co-ordinate the development of Server room standards.

21.3.11. The Director of Technology and Information will co-ordinate measures to ensure that a reliable power supply to the server room is in place and that adequate safeguard are there to protect the equipment.

21.3.12. No drinking, eating or smoking is allowed in the server room.

21.3.13. Water alarms must be installed to detect water leakage in the server room.

21.3.14. The power distribution box in the server room must be linked to batteries providing temporary power to operate the devices in the room until the necessary alternative power source is obtained.

21.3.15. The power distribution box in the server room must be linked to a power generator that works immediately upon power interruption to ensure uninterrupted power is provided to the devices in the room, including air conditioning and detectors.

21.4. Responsibilities

Director of Technology and Information and Information Security Officer.

22. MAGNETIC MEDIA POLICY

22.1. Purpose

This policy discusses the requirements for the handling of Magnetic media.

22.2. Scope

This policy is applicable to all media, i.e. Hard Disk, Compact Disc, Floppy Disk, Laser Disk, Magnetic Tape Reel, Magneto-Optical Disk, Zip Disk, Magnetic Tape Cartridge and Digital Audio Tape.

22.3. Policy

22.3.1. An inventory of all critical magnetic media should be maintained and kept in the secure magnetic media library.

22.3.2. All magnetic media should be properly labelled.

22.3.3. All magnetic media should be physically destroyed prior to discarding.

22.3.4. The shelf life of all media should be ascertained from the respective vendors and should be monitored.

22.3.5. All media should be scanned for viruses prior to use.

22.3.6. In the event of deciding to re-use the equipment or media by other employees or by someone outsourced, the previous data must be labelled "Safe".

22.3.7. Documenting all the items that have been disposed of, whether by sale, removal or destruction by registering the asset numbers in the IT assets inventory.

22.4. Responsibilities

Director of Technology and Information and Information Security Officer.

23. SERVER SECURITY POLICY

23.1. Purpose

This security policy discusses the issue of securing the internal servers of GCC-STAT. This is to make sure that there is no unauthorized access to GCC-STAT information.

23.2. Scope

This policy applies to all servers operated by GCC-STAT.

23.3. Policy

23.3.1. The Servers should be located in a physically secure place.

23.3.2. All configurations of the servers should be documented and approved by the Director of Technology and Information.

23.3.3. Each server should have documentation of configuration, operating system version, patches installed, backup and recovery procedure.

23.3.4. All Change Management Policies should be strictly implemented on the servers.

23.3.5. The Director of Technology and Information should approve all configurations of servers.

23.3.6. Services not required, such as the web server and others, should be disabled.

23.3.7. The Log of the server should be monitored on a semi-annual basis, as specified by the Information Security Officer.

23.3.8. All security patches should be installed on the server after confirmation that they will not have any adverse effect on the running applications.

23.3.9. All guests and default accounts will be either disabled or their password changed.

23.3.10. If remote management of the server is required, a secure channel should be used for this purpose.

23.3.11. The privileged account like administrator and root should only be used when required.

23.3.12. A regular Audit would be performed by the Information Security Officer.

23.4. Responsibilities

Director of Technology and Information, Information Security Expert, Systems Administrator and Information Security Officer.

OPERATIONS MANAGEMENT POLICIES

24. CONFIGURATION MANAGEMENT POLICY

24.1. Purpose

This security policy deals with proper documentation for the configuration of critical systems.

24.2. Scope

This policy applies to all servers, network equipment and others, either owned or operated by GCC-STAT.

24.3. Policy

24.3.1. All system configurations, including hardware, software and core business software should be documented.

24.3.2. There should be a hard copy and a soft copy of the documentation.

24.3.3. The documentation should contain a configuration baseline. All changes from this baseline should be documented as per Change Management Policy.

24.3.4. Prior to roll out, any modification made to the default configuration should be documented in the configuration management documentation.

24.3.5. The Director of Technology and Information should approve all configurations Documentation.

24.3.6. Configuration management and change management documentation should be used together, in case of recovery.

24.4. Responsibilities

Systems Administrator, Director of Technology and Information.

25. CHANGE MANAGEMENT POLICY

25.1. Purpose

This security policy sets out the proper change management documentation for the all critical systems.

25.2. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by GCC-STAT.

25.3. Policy

25.3.1. Standardized methods and procedures should be used for the efficient and prompt handling of the changes and revision control.

25.3.2. All changes should be documented and prior approval must be obtained for all changes made to critical production systems.

25.3.3. A "Change Request" should be presented to the relevant manager for approval. The Director of Technology and Information will co-ordinate the work-flow for change approval.

25.3.4. All requested changes should be evaluated by the IT Team and have their impact assessed before approval or disapproval.

25.3.5. All changes, once approved, should be scheduled in such a way as to ensure the availability of a time slot for a rollback, should something unexpected happen.

25.3.6. Documentation for a change request should be accompanied by detailed, step-by-step procedures to do the change. It should also include detailed roll back procedure, in case the change fails and desired result is not achieved.

25.3.7. Whenever there is a need to change the application software, system software, LAN or any hardware, the change should be appropriately authorized and approved.

25.3.8. Every change should be thoroughly tested and fully documented.

25.3.9. Changes should be made when there is minimum or no activity on the system. In case, where there is more than one change to be carried out at a given time, the changes should be queued on the basis of business and technical priority.

25.3.10. Changes should only be approved after adequate consideration of the associated impact and implications.

25.3.11. Changes, once accepted, should be entered into the Change Management Log and Documented.

25.3.12. The Change should be fully tested and the result presented to the respective manager.

25.3.13. A Change Management Summary report should be presented to higher management on a Monthly Basis.

25.4. Responsibilities

Director of Technology and Information, Systems Administrator, Network Administrator.

26. PRINTED OUTPUT AND DISTRIBUTION POLICY

26.1. Purpose

This security policy sets out the requirements for printed output and its distribution.

26.2. Scope

This policy applies to all critical reports generated or dealt by GCC-STAT.

26.3. Policy

26.3.1. The dissemination policy adopted by the GCC-Stat must be applied.

26.3.2. Safe disposal of the waste papers of confidential outputs and publications.

26.4. Responsibilities

Report Printing Users, Information Security Officer.

27. GENERAL BUSINESS CONTINUITY POLICY

27.1. Purpose

The purpose of this policy is to provide directions regarding business continuity.

27.2. Scope

This policy applies to all business critical systems as referred to in the Business Impact Analysis and Risk Assessment in the GCC-STAT Security Policy after the completion of the infrastructure.

27.3. Policy

27.3.1. The Director of Technology and Information will ensure that the availability of the business-critical system is ensured as per the Risk Assessment requirement of the GCC-STAT Policy.

27.3.2. Critical system must have recovery procedures that can be depended upon in case of disasters.

27.3.3. The word “Disaster” needs to be defined and the respective risk evaluated by senior management. The Director of Technology and Information should coordinate this task.

27.3.4. All documentation related to business continuity should be regularly updated.

27.3.5. The Director of Technology and Information will ensure that there is an appropriate Contingency plan, and "Emergency Response Plan” are in place.

27.4. Responsibilities

Risk Manager, the Director of Technology and Information Departments Directors and Information Security Officer.

28. BACKUP AND RECOVERY POLICY

28.1. Purpose

This security policy specifies the backup and recovery standards for GCC-STAT.

28.2. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by GCC-STAT.

28.3. Policy

28.3.1. Backup of all critical devices, including the server, communication equipment and mission-critical hardware and software, should be undertaken.

28.3.2. Frequency of the backup will be decided according to the nature of the application being used.

28.3.3. The preferred backup method is "Full Backup" followed by a "Differential backup".

28.3.4. Unless there is justification, the “Incremental Backup” method should be avoided because in the case of a data recovery, one backup failure may make the entire backup process fail.

28.3.5. When storing historical data, the shelf life of the media should be considered.

28.3.6. The timing of "Distributed Backups" should be planned to have the minimum impact on the GCC-STAT corporate network.

28.3.7. The backup process should not violate the confidentiality of the system

28.3.8. No public computers should be used for backing up sensitive data.

28.3.9. All archive data must be tested on 2 years basis.

28.3.10. All backups should be verified to check the validity of the media. The “Read after Write” option should be chosen, where available.

28.3.11. In the case where distributed backup agents are not available, business-critical data should be put in a directory on the server to be backed up. Director of Technology and Information will make the necessary arrangements.

28.3.12. The Information Security Officer, in consultation with the Director of Technology and Information, will make arrangement for Electronic Vaulting i.e. storing of the backup data at an off-site location.

28.3.13. Once the backup media is no longer usable, it should be physically destroyed or preferably burnt.

28.4. Responsibilities

Systems Administrator, Network Administrator, Director of Technology and Information.

29. PERSONNEL POLICY

29.1. Purpose

This security policy specifies guidelines and standards related to Human Resource (HR) with special reference to Information Security.

29.2. Scope

This policy applies to all permanent and contract employees.

29.3. Policy

29.3.1. Prior to hiring a prospective employee, HR must do a background check, contact references and validate the education testimonial.

29.3.2. Employees should sign the undertaking accepting responsibility for adherence to security policies.

29.3.3. HR will ensure that security responsibility is included in the job responsibilities of the employee.

29.3.4. The Terms and Conditions of employment shall mention the Information Security policy for each employee

29.3.5. HR will ensure that segregation of duties and job rotation is implemented, where possible.

29.3.6. When an employee leaves the employ of the company, HR will ensure that an exit interview is conducted.

29.3.7. HR will ensure that the person has all computer accounts removed prior to his/her final settlement.

29.3.8. In the case where employment is terminated without the consent of the employee, he/she should be escorted from the premises.

29.4. Responsibilities

HR Department and Information Security Officer.

30. THIRD PARTY POLICY

30.1. Purpose

This security policy specifies the standard and guidelines for the third party and outsourcing.

30.2. Scope

This policy applies to parties whether they are vendors, contractors, consultant or outsourced professionals.

30.3. Policy

30.3.1. The Risks associated with third party involvement and outsourcing should be identified and appropriate measures taken to address them.

30.3.2. A Non-disclosure agreement is essential before sensitive information is shared with a third party.

30.3.3. The role and responsibilities of the third party should be clearly defined.

30.3.4. Third party access to the GCC-STAT corporate computer system will be given only after the signing of a formal contract, which should contain all security requirements by which the third party is to abide.

30.3.5. All Third party and external users, if defined on the system, should have a mandatory expiry date.

30.3.6. Third party or outsourced tasks, which require communication privileges, should be restricted and monitored.

30.3.7. Information assets protection procedures and full retrieval of information must be followed.

30.3.8. Clear identification of the service provided by third party and the information of security level must be followed.

30.3.9. Well-defined constrains on information copying and disclosure (The non-disclosure document), clearly specified.

30.3.10. The statement of intellectual property rights and the GCC-Stat's eligibility to monitor, audit and cancel and privileges or powers granted to the third party if it was proved that it did not adhere to security rules, and to cooperate with the Oman National Computer Emergency Readiness Team (CERT) with regard to security incidents.

30.4. Responsibilities

Director of Technology and Information, Finance & HR Manager and Information Security Officer.

31. MOBILE DEVICE SECURITY POLICY

31.1. Purpose

This security policy specifies the standard and guidelines for the mobile devices

31.2. Scope

This policy applies to all GCC-STAT employees, contractors, consultant or outsourced professionals.

31.3. Policy

31.3.1. All mobile devices should be registered with MDM and access approval should be obtained from Director of Technology & Information

31.3.2. Mobile Device Management (MDM) system must support all kinds of Mobile Operating Systems

31.3.3. MDM should be controlled either through web or by a single console

31.3.4. All data including in-transit and at-rest and content sent to mobile devices must be encrypted

31.3.5. End- to End Mobile security must be ensured in terms of User, Devices, Applications, Content, Data, Email and Network Levels.

31.3.6. Mobile device users shall be authenticated and authorized by using their Active Directory credentials

31.3.7. All mobile users must trained on to physical protection of their mobile phones and report to Information Security Officer, in case of their device is stolen or broken

31.3.8. Ensure MDM system should support in sending message to any device, lock, find, remote view, sync, device wipe

31.3.9. Inactivity timeout shall be set. The recommended inactivity timeout is 15 minutes but must not exceed 60 minutes

31.3.10. MDM shall prevent data loss on user authentication, data encryption, data backup restrictions and compliance tracking.

31.3.11. All attached storage cards that contain Legally Restricted Information must be destroyed or wiped so no data recovery is possible.

31.3.12. It is impermissible to allow mobile phones with recording devices to access highly controlled areas without the prior approval of the Director of Technology and Information.

31.3.13. Unregistered mobile devices should not be connected to the GCC-STAT system devices, or allowed to store the GCC-STAT hardware data. Mobile and laptops are allowed to connect to the GCC-STAT network on a temporary basis provided that they are disconnected from the main networks by firewalls.

31.3.14. It must be ensured that mobile phones are GPS enabled and can be remotely controlled in case they were lost or stolen by sending warnings to their carriers that they need to deliver them to the concerned authorities, or to disable them and destroy the entire contents, in case it was difficult to retrieve them.

31.4. Responsibilities

Director of Technology and Information and Information Security Officer.

32. SECURITY INCIDENT MANAGEMENT POLICY

32.1. Purpose

The Security Incident Response and Management Policy is developed to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

32.2. Scope

This policy applies to GCC-STAT's all information assets, permanent and Contract personnel, business partners, and contractors dealing with GCC-STAT

32.3. Policy

Detection and Initial Reporting

32.3.1. 'Incident' is a term related to exceptional situations or a situation that warrants intervention of each Department's Director. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing security policies and procedures of GCC-STAT thus impacting the confidentiality, integrity and availability of information. An incident may relate to any of the following:

- Suspected hacking attempts
- Successful hacking attempts
- Hardware resources and components lost / stolen
- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Failure / crash of IT equipment
- Power problems
- Natural calamity or disaster

32.3.2. An incident may be detected by anybody in the organization. The concerned personnel shall immediately bring it to the notice of the Department Director. The Director shall intimate the facts to the Information Security Officer by filling the Security Incident Form or send email to securityincident@gccstat.org

Documentation

32.3.3. Information Security Officer shall, in consultation with the Director(s), analyze the impact of the incident. Information Security Officer shall maintain the central database of all such incidents and shall communicate the details to Information Security Steering Committee or to the DG.

32.3.4. Where an incident is escalated to a level that necessitates legal action to be taken, adequate evidence shall be gathered and retained to adhere to the rules for evidence as stipulated by the relevant regulation/jurisdiction.

32.3.5. A detailed risk and impact analysis for the incident shall be carried out by the Information Security Officer to have a preventive and corrective control in place.

Monitoring

32.3.6. All the major security incidents shall be reviewed by Internal Audit Department and discussed in the subsequent Information Security Steering Committee meetings or to the DG.

Development of Corrective Action Plan

32.3.7. Information Security Officer in consultation with respective Director shall prepare the corrective action plan for the incident. The action plan, though specific to each case, shall typically cover the following:

- Particulars about the date and description of the incident
- Facts and explanation / reasons for the incident
- Impact of the incident
- Other business units affected
- Corrective action to be taken
- Estimated cost and time frame for implementing the corrective action, start date and end date
- Personnel responsible for taking the action

32.4. Responsibilities:

Directors, Internal Auditor(s) and Information Security Officer.

33. AUDIT AND COMPLIANCE POLICY

33.1. Purpose

The Audit, Compliance and License Management Policy is developed to detect and avoid breaches in any criminal law, statutory, regulatory or contractual obligations and of any security requirements. It is also designed to ensure compliance with organisations security policies and standards.

33.2. Scope

This policy applies to GCC-STAT's all information assets, permanent and Contract personnel, business partners, and contractors dealing with GCC-STAT

33.3. Policy

33.3.1. The following logs/information shall be reviewed on a regular basis:

- Critical server logs
- Network/security devices logs
- Access rights and requests
- Compliance to mobile device security policy
- Compliance to information security policies and procedures

33.3.2. The process of finding out the new threats/exploits related to the organization's information security shall be continuous. The following activities shall be at least once a year.

- Vulnerability Assessment
- Penetration Testing
- Technical Audit

33.3.3. Compliance with copyrights shall be met.

33.3.4. All purchased software shall follow the license management procedure.

33.3.5. Information Security Officer or Internal Auditor shall conduct an audit by random sampling and checking of paper licenses every six months.

33.3.6. The licenses for operating systems (HP-UX, Linux, and Windows etc.) shall be under the custody of Director of Technology and Information.

33.3.7. Licenses for application software shall be maintained by respective application owners within the Department of Technology and Information.

33.4. Responsibilities

Director of Technology and Information, Internal Auditor(s) and Information Security Officer.

Technology and Information Department – Main Positions

Position	Employee Name
Director Technology and Information	Eng. Mubarak Al Sulti
Expert, IT	Elham Saleh
Head, Information System	Eng. Fahad M. Senan
Information Security Officer	Rajesh Ramamoorthy
Consultant, IT	Nalakha Kumarasinghe
System Analyst	Khulood Al Busaidi
Administrator, Systems & Network	Gayan Kularatne