POLICIES & PROCEDURES

SECTION: **INFORMATION TECHNOLOGY SECURITY**	
PREPARED BY: IT Manager	IMPLEMENTED DATE: 01 JAN 2015
APPROVED BY: GROUP CEO	REVISED ON: 01 DEC 2014
COMMUNICATE TO: Dept Heads, Group Finance and Accounting	

APPROVAL FOR BELOW POLICY AND PROCEDURE

1. IT-ITSP-PP001 - IT Security Policy

Kiran Vaidya
Corporate Finance Director
Date 12 AUG 2015

Prabsharan Singh Thakral
Group Chief Executive Officer
Date 12 AUG 2015

BOUTIQUE
Group of Companies
AFFILIATES OF THAKRAL LAND

Boutique Group of Companies

Information Technology Security Policy

Document Review and Approval

Revision History

Version	Author	Revision Description	Date
1.0	Mahdee Boonmalert	Initial release	1st December 2014

This document has been reviewed by

S/N	Reviewer	Date reviewed
1	Ameya Deepak Gogate	29/7/15

This document has been approved by

S/N	Approver	Date approved
	PRAB THAKRAL	

Table of Contents

Introduction

Information in IT Systems is an asset, like other important business assets, has value and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure operations continuity and minimize business damage and maximize return on IT investments.

Boutique Group of Companies (BGC) information systems landscape comprises of a broad range of information systems from personal Internet/Intranet web servers to highly sensitive and critical corporate systems. The systems have different characteristics in the following key areas:

- Sensitivity of information
- Criticality to operations of the Company and Departments
- Risk exposure
- Potential damage to the BGC in the event of a security breach
- Security management responsibility

The implementation and management of the security of this diverse range of systems, with varying security requirements, throughout the entire system life cycle, will be addressed by BGC IT Security Policy.

The Policy defines security measures so that BGC information assets are adequately protected and consistency in the implementation and practice of security throughout BGC can be achieved.

1. Information Security Policy

***Objective**: To provide management direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.*

1.1 Definition of Information Security

1.1.1 The objective of this Information Security Policy Manual is to establish the Information Security Management Systems (ISMS) which would provide a framework of security policies to protect BGC IT assets and resources from unauthorized access, accidental or intentional disclosure and destruction so as to minimize disruption to business activities.

1.1.2 Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an IT security policy across the organization.

- **Confidentiality**: Ensuring that information (either owned by or shared with BGC) is accessible only to authorized personnel.
- **Integrity**: Safeguarding the accuracy and completeness of information (either owned by or shared with BGC) and processing methods.
- **Availability**: Ensuring authorized users have access to information and associated assets (either owned by or shared with BGC) when required.

1.1.3 BGC shall implement a range of suitable controls to achieve information security, including specific policies, practices, procedures, organizational structures and software functions.

1.2 Statement of Management Intent

1.2.1 The BGC Management realizes the importance and value of its information systems and its processing resources, both manual and automated. Taking account of this importance the management of BGC is committed ensuring the confidentiality, integrity and availability of its information systems and to take the necessary action to ensure that suitable controls are in place to provide an adequate level of protection.

1.2.2 The BGC Management provides full support for the development and implementation of policies, procedures and controls. BGC management ensures that these policies, procedures and supporting documentation, will be subject to a review process and appropriate ongoing development.

1.3 Responsibility for Security

1.3.1 BGC and all business units are responsible for complying with BGC information security standards as defined in BGC IT Security Policy.

1.3.2 BGC personnel comply with applicable policies and procedures for safeguarding any BGC information technology asset in their control against theft, loss and misuse.

1.4 Compliance

1.4.1 All BGC IT staff shall comply with this policy and the standards spelled out in this manual.

1.4.2 IT Manager will be responsible to ensure that IT staff are aware of their day-to-day security responsibilities as well as this corporate policy and any operation policies and procedures that might apply for securing information systems.

2. Organizational Security

2.1 Information Security Infrastructure

Objective: *To manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management with management leadership should be established to approve the information security policy, assign security roles across the organization.*

2.1.1 Authorization Process for information processing facilities

2.1.1.1 Authorization Process for New Information Technologies

- The IT Manager should recommend new information technologies for e.g. computer hardware or software, ensuring all relevant security policies and requirements are met. The approval process for such facilities shall be in accordance to ***IT-HSM-PP001 (Computer Hardware & Software Acquisition)***
- All personal mobile computing equipment, not limited to employee owned computers and PDA, shall not be used for processing business information, unless authorized by direct supervisor or Group Finance and Accounting or Group CEO.
- All personal mobile computing equipment, not limited to employee owned computers and PDA, must complete **IT-HSM-PP005 (Personal Device Register From)** before access to company network.

2.1.2 Co-operation between organizations

2.1.2.1 Contacts to appropriate external authorities shall be maintained with regards to security as appropriate for BGC employees and their roles. This includes Internet Service Providers (ISPs), telecommunications companies and other regulatory organization. All communications between BGC and these third parties shall be maintained in confidentiality when appropriate.

2.1.3 Information Security Responsibilities

2.1.3.1 All information is owned by individual business units, not by information technology department. The manager of the business unit responsible for the creation of any data and/or the business unit directly impacted by the loss of that data is the Information Owner. Responsibilities include, but are not limited to:

- ensuring security controls in place;
- reviewing and ensuring appropriate access rights for the staff accessing the system;

- determining back up requirements for the information they own; and
- taking appropriate action on security violations.

Information Technology department will coordinate for technical support to each department manager.

2.2 Security of third party access

Objective: *To maintain the security of organizational information processing facilities and information assets accessed by third parties. Access to the organization's information processing facilities by third party should be controlled.*

2.2.1 Third party security requirements

2.2.1.1 Third parties may be required to locate on-site for a period of time as defined in the contract. On-site third party includes, but not limited to,

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and other outsourced support services
- Contract and temporary staff
- Consultants

2.2.1.2 Access to the organization's information processing facilities by third parties should be controlled. Security risks with regards to physical and logical access into the organization should be considered.

2.2.1.3 All third parties are recommended to enter into a formal agreement stating the security requirements with the following considerations:

1. Information handling arrangement
2. Target level of acceptable service
3. Liabilities of the parties
4. Intellectual property rights (IPR) and copyright protection of collaboration work
5. Physical and logical (including privileges) access control arrangement
6. Requirement to maintain a list of individuals that are authorized to use the service and their privileges
7. Right to monitor and revoke user activity
8. Right to audit contractual responsibilities or audits carried out by a third party
9. Restriction on copying and disclosing organization information
10. Return or destruction of all information upon the end of the contract
11. Requirement to protect against malicious software
12. Involvement of third party with subcontractors

2.3 Outsourcing

***Objective**: To maintain the security of information when the responsibility for information processing has been outsourced to another organization. Outsourcing arrangement should address the risks, security controls and procedures for information systems, networks and desktop environment in the contract between parties.*

2.3.1 Outsourcing Security Requirements

2.3.1.1 Staff engaging outsource service shall ensure the stated security requirements are the same or stronger than the policy requirements.

2.3.1.2 All outsourcing is recommended to enter into a formal agreement stating the security requirements.

2.3.1.3 Contractors shall sign confidentiality agreement on award of contract, either at individual or company level depending on the circumstances.

3. Asset Classification and Control

3.1 Accountability for assets

Objective: *To maintain appropriate protection of organizational assets. All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained.*

3.1.1 Inventory of assets

3.1.1.1 An asset inventory associated with information systems shall be maintained by IT Department and reviewed bi-annually. The asset inventory is recommended to contain information such as asset type, asset information, purchase date and owner/responsible party.

3.1.1.2 Information shall be classified by the owner to indicate the need, priorities and degree of protection. The information system asset is recommended to include but not limited to the following:

- Computer Hardware and Peripherals
- Network Devices
- Communication Devices
- Application Software
- Operating System
- Database

4. Personnel Security

4.1 General Responsibilities

***Objective**: To reduce the risks of human error, theft, fraud or misuse of facilities.*

4.1.1 Security is the responsibility of all employees and persons involved with BGC. Therefore, all employees, contractors, vendors, and persons with access to BGC facilities and information shall abide by the standards as documented and include security as one of their core job responsibilities.

4.2 User Training

***Objective**: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work. Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.*

4.2.1 Information Security Education and Training

4.2.1.1 All employees of the organization and, where relevant, third party users, shall receive appropriate training and regular updates in organizational policies and procedures where possible.

4.2.1.2 The training shall include general awareness training as well as specific training as according to the job scope.

4.2.1.3 New Employee Orientation: Upon permanent or contract employment at BGC, all staff members are to be briefed on the application of information system security policy and procedures within the company. Components of security awareness training are recommended to include, but is not limited to:

- Personnel security
- Security incident reporting and elimination
- Compliance
- E-mail use guidelines
- Information security monitoring processes in use
- Whom to contact for additional information
- Awareness to social engineering techniques employed by hackers

4.3 Responding to security incidents and malfunctions

***Objective**: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents. Incidents affecting security should be reported through appropriate management channels as quickly as possible.*

4.3.1 Channels for reporting security incidents and weakness shall be established in accordance to ***IT-SEC-PP002 - Security Breach Reporting & Management Procedure***. The organization should learn from the incidents to prevent future occurrences.

5. Physical and Environment Security

5.1 Secure Areas

***Objective**: To prevent unauthorized access, damage and interference to business premises and information. Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.*

5.1.1 Physical security perimeter

5.1.1.2 BGC facilities requiring enhanced physical security shall have its own physical security perimeters. Critical or sensitive business information processing facilities shall be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage and interference. This refers to computer room.

5.1.2 Fire Safety

5.1.2.1 No smoking shall be allowed within computer room.

5.1.2.2 Combustible material should be removed from critical areas.

5.1.2.3 Smoke detectors and other fire detection devices should be installed. Regular checking on these devices should be done.

5.1.3 Securing Offices, Rooms and Facilities

5.1.3.1 Physical access to all computer rooms shall be tightly controlled. Doors shall be locked at all times with only authorized personnel having the access. Access rights to computer room should be regularly reviewed and revoked immediately once it is no longer needed.

5.1.3.2 All visitors to the computer room shall register themselves with in the log book before entry.

5.1.3.3 A visitor's log shall be maintained to keep track of visitors to the computer room. Recommended fields in the log are name, company, date, time of entry and departure, reason for the visit and name of escorted staff.

5.1.3.4 IT equipment should be physically protected when not in use.

5.1.3.5 Any hazardous or combustible materials shall be stored at a safe distance from any secure area.

5.1.3.6 Rooms containing wiring or communications equipment (wiring closets, PBX rooms, etc.) shall be locked at all times with access restricted to authorized personnel only.

5.1.3.7 To avoid unnecessary access and damages, computer facility rooms shall not be used for printing, faxing, or other non-concern routine operations.

5.1.3.8 Computer facility rooms shall not be shared with third parties.

5.1.3.9 Backup and recovery media and facilities shall be located at a safe distance from main facilities. The backup facilities shall be at a distance that would protect it from damage from any incident at the main site.

5.1.4 Working in Secure Areas

5.1.4.1 For all maintenance personnel/visitors wish to work in the department, they shall be authorized and can produce the appropriate identification and at all times should be accompanied by authorized personnel.

5.1.4.2 Any third party access granted to computer room shall be strictly controlled and monitored. All parties with access to the area shall be authorized and logged. This includes support services such as cleaning or waste removal.

5.1.4.3 Access to critical areas shall be granted on a need-to basis. Only authorized personnel shall enter the computer room.

5.1.4.4 Photographic, video or audio equipment shall not be allowed in critical areas, unless authorized.

5.1.4.5 Critical operator actions like network reconfiguration and patching should be supervised.

5.1.5 Security in Delivery and Loading Process

5.1.5.1 All IT equipments deliveries should be pre-arranged and registered on entry and record by IT staff.

5.2 Equipment security

***Objective**: To prevent loss, damage or compromise of assets and interruption to business activities. Equipment should be physically protected from security threats and environmental hazards.*

5.2.1 Equipment siting and protection

5.2.1.1 All BGC equipment shall be sited in a manner or location to minimize risks or threat. This includes, but is not limited to:

- threats of theft or vandalism
- risk of fire, explosion, smoke, chemical agents
- loss of services such as power, communication or water
- Any other physical threat.

5.2.1.2 All smoking, drinking and eating in computer room shall be disallowed.

5.2.1.3 Computer equipment shall be housed in an environment equipped with fire detection and prevention measures.

5.2.1.4 Critical equipment should be located in non-public areas and in a secure room. Access to critical equipment should be limited to authorized staff only.

5.2.2 Power Supply Protection

5.2.2.1 To avoid power failures, a suitable electrical power supply shall be provided in such way that Single Points of Failure can be avoided. Based on system criticality, the use of a back-up generator shall be considered.

5.2.2.2 Uninterruptible Power Supplies (UPS) is strongly encouraged to be used for equipment supporting critical operations to orderly shut down or allow systems to continue running. UPS equipment shall be checked regularly to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

5.2.3 Network Cabling Protection

5.2.3.1 All power and telecommunications equipment and cabling shall be protected against deliberate or accidental interruption of service.

5.2.3.2 Cabling shall be performed by authorized personnel only and shall be physically and electrically tested before commissioning.

5.2.4 Equipment maintenance

5.2.4.1 All equipment shall be correctly maintained to provide availability and protect the integrity and confidentiality of information. In accordance with manufacturer's specifications, equipment should be monitored and inspected. Only authorized maintenance personnel are allowed to perform repairs and all repairs or service work shall be recorded. If equipment shall be sent offsite for repairs, the confidentiality and integrity of any information shall be ensured.

5.2.5 Security of equipment off-premises

5.2.5.1 Approval from Management has to be obtained before moving equipment off-premises for information processing

5.2.5.2 Manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields.

5.2.5.3 Staff should not leave the equipment unattended.

5.2.6 Secure disposal or re-use of equipment

5.2.6.1 Prior to equipment disposal or reuse, any BGC information processing equipment shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten.

5.3 General controls

***Objective**: To prevent compromise or theft of information and information processing facilities. Information and information processing facilities should be protected from disclosure to, modification of or theft by unauthorized persons, or controls should be in place to minimize loss or damage.*

5.3.1 Clear Desk and Clear Screen Policy

5.3.1.1 All PC and computer terminals shall have a password protected screen saver or other controls activated after a period of inactivity (recommended period is 15 min).

5.3.1.2 Staff shall ensure that confidential IT documents shall not be left unattended on their tables at end of each working day or when absent from the desk for a long period of time.

5.3.2 Removal of Property

5.3.2.1 Employees or contractors shall not remove IT property off BGC premises, without prior authorization. All individuals shall be aware that spot checks can take place. All equipment that is removed shall be logged out and logged back when returned.

6. Communication and Operations Management

6.1 Operational Procedures and Responsibilities

Objective: *To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures.*

6.1.1 Documented Operating Procedures

6.1.1.1 Documented operating procedures are to ensure correct and secure operations. As such, changes within the documents shall be authorized by IT Manager. These documents shall contain specific instructions on processing and handling information. If service or application involves any external parties, all contact information for operational or technical difficulties shall be included in the documentation. Documents that are documented in IT Policies and Procedures are for the relevant areas and should be modified when necessary to localize it.

6.1.2 Operational Change Control

6.1.2.1 A change management procedure shall be established to control all addition, deletion and modification to the system, networking devices, software or similar devices.

6.1.2.2 All requests to implement any system/network or software change shall follow the change management procedures according to ***System, Network and Software Application Change Management Policy (IT-CMT-PP001 and IT-CMT-PP002)*** respectively.

6.1.3 Incident management procedures

6.1.3.1 All incidents have to be reported to the appropriate parties, the incident shall be escalated for investigation.

6.1.3.2 An incident management procedure shall be established to manage security incidents in quick and effective manner. Refer to ***IT-CMT-PP002 - Software Application Change Management***.

6.1.3.3 Security incidents will be investigated by IT Department to determine the severity of the incident and identified by the levels defined by this policy. Investigative methods and procedures will be used based upon the Severity level. Security violations will be followed by corrective action by management.

Severity 1 - An event that is, or could become a serious and immediate threat to any of the devices on BGC network and requires immediate attention and action. Threatened devices may include routers, networks, servers, firewalls, network management hosts, attached LAN's, or user hosts.

Severity 2 - An event that is, or could become, a future threat, but which has not been determined as serious enough as of that time. Hence, it may or may not require an immediate response depending on the incident.

Severity 3 - An event that is, or could become, a minor annoyance or threat; or which has been determined to be a non-threat resulting from either authorize, or unauthorized network activity. Severity 3 events are informational in nature and can be acted upon at a later time.

6.1.4 Segregation of Duties

6.1.4.1 Controls shall be deployed to mitigate any activities that would circumvent any procedural restrictions or business process operations. Any activity that could result in fraud or misuse of information systems shall have mitigating controls for separation of duties or the implementation of controls to detect fraud or misuse.
For e.g. segregation between software development and system operations.

6.1.5 Separation of Operational and Development Facilities

6.1.5.1 Separate, controlled environments shall exist for development, user acceptance testing, and production where possible.

6.1.5.2 The production environment is where the production executable code for an application will reside. Only an authorized engineer will have write access to these libraries. Application developers are not allowed to move code into the production environment.

6.1.5.3 Compilers or other system development tools shall not be installed on production machines. All code shall be precompiled before moving into a production environment where applicable. If a compiler or any system development tools are necessary on a production machine, appropriate approval has to be obtained.

6.1.6 External facilities management

6.1.6.1 All operational processes performed by external or third parties shall have appropriate controls and approvals from application/system owners.

6.1.6.2 Outsourced facilities management should possess better, if not the same, security controls.

6.2 System planning and acceptance

***Objective**: To minimize the risk of system failures. Advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirements should be made, to reduce the risk of system overload.*

6.2.1 Capacity Planning

6.2.1.1 All information systems shall meet anticipated capacity requirements. It is the responsibility of the system's development and operational teams to determine anticipated hardware requirements and capacity and monitor system capacity performance. This includes, but is not limited to:

- Disk usage and size
- Network traffic load
- Load balancing
- Necessary processing power
- Necessary memory requirements

6.2.2 System Acceptance

6.2.2.1 All systems shall have acceptance criteria for new development and new major enhancement. The criteria shall be clearly defined, agreed, documented and tested.

6.2.2.2 All system acceptance testing shall be signed off using ***IT-CMT-PP002 - Software Application Change Management.***

6.3 Protection against malicious software

***Objective**: To protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious software.*

6.3.1 Controls against malicious software

6.3.1.1 BGC supplied virus screening software shall enable on all computers and updated regularly. It is the responsibility of the end user to ensure

this process is running on their assigned laptops or desktops. If the user has any reason to believe the process is not running properly, he/she should report to the IT Department.

6.3.1.2 E-mail attachments and files downloaded from the Internet shall be scanned before execution. External storage media (USB disk, etc.) that have been out of the control of the user shall be scanned before use.

6.3.1.3 All virus detected, configuration changed, abnormal behavior of a computer or application shall be reported to the IT Department immediately.

6.3.1.4 If a virus is suspected on a system, the employee shall disconnect the system from the network and notify IT Department immediately. He/she will work with IT Department to remove the virus prior to any re-connection to BGC network.

6.3.1.5 All staff shall not install and run software obtained from unidentified sources unless endorsed by IT Department.

6.3.1.6 Only licensed software acquired from third party providers and verified public domain software are allowed to be installed and used within the environment.

6.4 Housekeeping

***Objective**: To maintain the integrity and availability of information processing and communication services. Routine procedures should be established for carrying out the agreed back-up strategy taking back-up copies of data and rehearsing their timely restoration, logging events and faults, where appropriate, monitoring the equipment environment.*

6.4.1 Information Backup

6.4.1.1 Systems (including PC, server and notebook) should be regularly backup. PC and notebook users are responsible for their own backup. Server backup will be handled by IT staff.

6.4.1.2 Each department shall ensure that all information related to their business on BGC servers is backed up consistently. It is the responsibility of each department to work with IT Department to ensure that all information is backed up and available to be restored in the case of an emergency.

6.4.1.3 Back-ups shall be stored in a safe, off-site, location and an appropriate level of physical and environmental protection shall be applied. All back-up brought offsite shall be recorded and documented.

6.4.2 Operator Logging

6.4.2.1 IT Operators should be aware that their activities will be monitored. Operational activity should be monitored, including login, logout, audit trail functions etc where technically possible.

6.4.2.2 Operation logs will be back-up and retained for investigation purposes if required.

6.4.3 Fault Logging

6.4.3.1 Operational personnel shall log all reports of errors or problems with information processing or communication systems in accordance to ***IT-FLM-PP001 - Server & Network Equipment Fault Logging & Maintenance***. The log shall include:

- date/time of fault
- equipment name
- description of error/problem
- name of party responsible for problem resolution
- description of problem resolution
- date/time of resolution

6.4.3.2 Fault logs shall be retained for investigation purposes if required.

6.5 Network Management

Objective: *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure. The security management of networks which may span organizational boundaries requires attention.*

6.5.1 Network Control Responsibilities

6.5.1.1 Logical layout of the network to be documented and should be kept up to date if and when changes occur.

6.5.1.2 Operational network controls shall be implemented. This includes:

- Proper availability for network operations and services
- Network should be monitored and managed.

6.6 Media handling and security

***Objective**: To prevent damage to assets and interruptions to business activities. Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media, input/output data and system documentation from damage, theft and unauthorized access.*

6.6.1 Management of removable computer media

6.6.1.1 All media, like diskettes, USB Drive, tapes and optical storage including printed reports, shall be stored in a secure manner to prevent theft.

6.6.1.2 All media should be clearly labeled.

6.6.1.3 Any computer media leaving the organization's facilities shall be authorized by appropriate management prior to leaving and an audit trail should be kept.

6.6.2 Disposal of Media

6.6.2.1 Electronic information storage devices (hard drives, tapes, floppies, CDs, etc) shall be disposed of in a manner that commensurate with the information stored there. Refer to ***IT-HSM-PP002 - Computer Asset Write Off & Disposal***

6.6.2.2 The proper destruction method for paper copies of confidential IT information is shredding or incineration.

6.6.3 Information Handling Procedures

6.6.3.1 Physical access to tape, disk, and documentation libraries shall be restricted to staff whose job responsibilities require access.

6.6.3.2 Manufacture specifications shall be met when storing any electronic media such as floppy disks, hard drives or CD-ROMS.

6.6.3.3 Recipients of data shall be clearly marked. Any media sent via interoffice mail, courier, or other means, shall be clearly labeled with the appropriate recipient information.

6.6.4 Security of System Documentation

6.6.4.1 System documentation shall be controlled and protected against unauthorized access. Access to the documentation shall be kept to a minimum and only individuals needing the documentation per their job

responsibilities will be given authorization. This documentation includes, but is not limited to:

- Operational procedures
- Network, system and application documentation
- Operations and production logs

6.7 Exchanges of information and software

***Objective**: To prevent loss, modification or misuse of information exchanged between organizations. Exchanges of information and software between organizations should be controlled, and should be compliant with any relevant legislation.*

6.7.1 Information and software exchange agreements

6.7.1.1 Controls shall be established over information and software exchange in order to ensure:

- Confidentiality of the information is maintained;
- The integrity of the information is maintained.

In order to safeguard the above while the information is outside BGC's security perimeter, the following will need to be considered:

- Software exchange agreements
- Security of media in transit
- Courier service or registered mail shall be the only recognized form of physical delivery
- Ownership of software and information shall be correctly spelt out in details.

6.7.1.2 Employees shall be conscious of disclosing confidential information in conversations or other forms of communication. This includes:

- Do not discuss confidential BGC information in public places
- Do not leave confidential information in voicemails.

6.7.2 Security of Media in Transit

6.7.2.1 Any information sent by postal service or courier shall be protected from unauthorized access, misuse or corruption. Employees are recommended to ensure packaging for information is sufficient to protect contents from physical damage or tampering.

6.7.3 Electronic Commerce Security

6.7.3.1 Web services shall be protected against intrusion using necessary access controls.

6.7.3.2 Terms and conditions shall be clearly defined for each e-commerce services launched including the terms of sales, pricing, fulfillment, maintenance, etc. Cryptographic techniques are recommended where appropriate.

6.7.4 Security of Electronic Mail

6.7.4.1 E-mail messages shall be considered to be the same as formal, written company memoranda. As such, email messages are considered part of company records and subject to monitoring, auditing and discovery acts. Therefore, when composing e-mail messages, users shall comply with all policies regarding the use of inappropriate language. Messages containing language that is in violation of policy will not be tolerated.

6.7.4.2 BGC employees shall not engage in any activities in connection with the Internet E-Mail System that is prohibited by BGC or this Policy or the terms and conditions of any internet access provider through whom BGC is procuring Internet access. Activities specifically prohibited include the following:

- Using the Internet E-Mail System for harassment purposes, whether through language, frequency, or size of messages.
- Sending of any malicious electronic mail, including, but not limited to, "mailbombing" (flooding a user or site with very large or numerous pieces of e-mail).
- Attempting to monitor, read, copy, change, delete or tamper with another employee's electronic communications without the consent of that employee (this does not apply to the BGC's authorized IT Department employee).
- Forging the source of electronic communications, altering system data used to identify the source of messages or otherwise obscuring the origin of communications.
- Sending chain letters or participation in any chain letter or pyramid schemes.
- Emails which contains defamation, wrongful discrimination, obscenity, fraudulent misrepresentation, abusive language

6.7.4.3 Email gateways connected to external networks shall have approved anti-virus software installed for the checking of incoming and outgoing mail attachments.

6.7.4.4 All internal names and IP addresses of the mail systems shall be hidden from the public Internet.

6.7.4.5 All emails that are sent externally should be appended by a trailer with the following text

This message is intended only for the personal and confidential use of the designated recipient(s) named above. If you are not the intended recipient of this message you are hereby notified that any review, dissemination, distribution or copying of this message is strictly prohibited. This communication is for information purposes only and should not be regarded as an offer to sell or as a solicitation of an offer to buy any financial product, an official confirmation of any transaction, or as an official statement of Boutique. Email transmission cannot be guaranteed to be secure or error-free. Therefore, we do not represent that this information is complete or accurate and it should not be relied upon as such. All information is subject to change without notice.

6.7.5 Public Available Systems

6.7.5.1 All requests for Internet server content hosting and future modifications shall be reviewed and approved by the authorized department before publishing the information to the public.

7. Access Control

7.1 Business requirement for access control

Objective: *To control access to information. Access to information/system, and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorization.*

7.1.1 Access Control Policy

7.1.1.1 Users shall be granted permission access data in accordance to ***IT/UAA/PP001/User Account Creation***. Authorization shall be documented via access request form, which shall be retained for historical purposes. Information/System Owners will grant access on a need to know basis, as required by job functions. Unnecessary access leads to unnecessary risk; therefore, a minimal approach shall be taken when assigning access to information.

7.1.1.2 Access to information shall be removed as soon as that access is no longer needed. It is the responsibility of both the user and the Information Owner to see that access privileges are aligned with the needs of the business and are assigned on a need to know basis. Refer to ***IT/UAA/PP02/User Account Deletion and Retention.***

7.1.1.3 Every user access to a multi-user system should be protected by a password to prevent unauthorized access.

7.1.1.4 System default guest accounts should be disabled.

7.2 User Access Management

Objective: *To prevent unauthorized access to information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services.*

7.2.1 User Registration

7.2.1.1 User registration and de-registration procedures shall be implemented when granting access rights for all information systems through User Account (Creation), ***IT/UAA/PP001*** and User Account (Deletion/Retention), ***IT/UAA/PP002*** respectively.

7.2.1.2 These procedures shall be documented and include:

- Proper authorization from authorized personnel to gain access to systems or information resources
- Sign off by requestor upon receipt of access
- Maintaining a record of all user registration history

7.2.1.3 All users of BGC computer systems shall be supplied with a unique user-id that is valid throughout the user's employment.

7.2.2 Privilege Management

7.2.2.1 The information/system owner is responsible for the user access rights to the service; with privileges sufficient only to fulfill their roles.

7.2.2.2 The information system owner shall ensure that the level of access granted is appropriate for the business purpose and does not compromise segregation of duties.

7.2.3 User Password Management

7.2.3.1 All access to computer systems shall be controlled by an authentication method involving a minimum of a Username/Password combination. The Username/Password combination should provide verification of the user's identity.

7.2.3.2 Where technically feasible, all passwords configuration shall follow Password Policy, ***IT/SPY/PP001/Password Policy***.

7.2.3.3 Unless authorized to the user, systems are recommended not to allow users to have multiple sessions on the same system.

7.2.4 User Access Rights Review

7.2.4.1 Information/System Owners are responsible for reviewing system privileges on a periodic basis and shall promptly revoke all privileges no longer required by users. User access rights reviews shall be performed on a half yearly basis where possible due to the ever-changing business environment and depending on the importance of the data. It is the responsibility of system administrators to ensure that Information Owners are provided with the proper reports to review current user access. Refer to ***IT/UAA/PP001/User Account Creation.***

7.3 User responsibilities

***Objective**: To prevent unauthorized user access. The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.*

7.3.1 Password use

7.3.1.1 All BGC employee shall safeguard their account logon ID and password information (such information will be assigned to single users and are not to be shared with any other person without authorization). The employee maybe held liable for any damage caused by the misuse of their account information.

7.3.1.2 Passwords shall be changed whenever there is any indication of possible compromise. Staff should change initial passwords immediately after the first successful access, if not prompted to do so by the system.

7.3.1.3 If employee is on leave or away for longer than 90 days, accounts can be disabled

7.3.1.4 Password must not be written on any documents or note in the notice area, such as post it on the working desk, monitor, etc.

7.3.2 Unattended user equipment

7.3.2.1 Appropriate security protection (e.g. password-protected screensaver with the automatic activation feature set at 10 minutes) should be installed into system or by locking (control-alt-delete for Microsoft Windows users) when their computer terminals are unattended to reduce unauthorized access opportunities when user equipment is not unattended for an extended period.

7.4 Network Access Control

***Objective**: Protection of networked services. Access to both internal and external networked services should be controlled.*

7.4.1 Policy on use of Network Services

7.4.1.1 Accessibility to network services should be restricted on a need-to-know basis and in accordance to the business requirement.

7.4.1.2 All systems should have access control mechanism to prevent unauthorized access.

7.4.2 External Network Connection

7.4.2.1 All BGC network connections to the Internet shall be protected by company firewall, to prevent unauthorized entry to BGC network.

7.4.2.2 BGC internal network addressing scheme shall not be visible to external connections. This keeps hackers or other external parties from easily gaining information about the structure of the networks and particular computers.

7.4.2.3 All external connections to internal network should be authenticated and through an approved application or security gateway.

7.4.2.4 All Internet access from internal is recommended to be directed through the proxy server.

7.4.4 Remote diagnostic port protection

7.4.4.1 All remote access points into BGC's environment shall be authorized and approved by IT Department. The use of non-authorized modems or remote access solutions is strictly forbidden and a violation of BGC security policy. Therefore, no unauthorized modems or remote access software may be used without the consent of IT Department.

7.4.5 Segregation in Networks

7.4.5.1 Internal network shall be protected with properly configured firewalls, and filtering routers when connected to external network where possible.

7.4.6 Network Connection and Routing Control

7.4.6.1 Firewalls shall be used to filter and control network connectivity between computer systems and the Internet.

7.4.6.2 Firewall shall protect against unauthorized access to internal resources. Control should be applicable to both incoming and outgoing transactions.

7.4.6.3 IT Department shall evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.

7.4.7 Internet Access Control

7.4.7.1 Internet accessibility is subjected to approval by Head of Department in ***IT/UAA/PP001/User Account Creation***.

7.5 Operating system access control

Objective: *To prevent unauthorized computer access.*

7.5.1 Terminal Log-On Procedures

7.5.1.1 Logon procedure shall display minimal information about the system. Successful and unsuccessful access shall be recorded where possible.

7.5.1.2 Systems shall be configured to not give any information on an unsuccessful login. This includes identifying which portion of login sequence (user-ID or password) was incorrect.

7.5.2 User Identification and Authentication

7.5.2.1 All users shall have a unique user id. The use of shared accounts or guest accounts should be subject to authorization. Each user account shall have an associated password known only to the approved owner.

7.5.3 Password Management System

7.5.3.1 Each user will be assigned with unique ID to maintain accountability.

7.5.3.2 Passwords shall be masked off during entry to the system. System shall force users to change initial passwords immediately after the first successful log-in where technically feasible.

7.5.3.3 System shall force the user to change the password when the password validity is close to expiry or expired where technically feasible.

7.5.3.4 System shall prompt the user to re-confirm the new password to prevent input errors during password change where possible.

7.5.3.5 Where technically feasible, all passwords configuration shall follow Password Policy, ***IT/SPY/PP001/Password Policy***.

7.5.4 Use of System Utilities

7.5.4.1 System utilities are available to enable system administrators to perform low-level maintenance tasks on a system. If inappropriate access is gained to these utilities they may be used to circumvent logical security controls. All utilities are recommended be:

- Be stored off-line if not required on a daily basis
- Have access restricted to a very limited group of authorized users

7.5.5 Terminal Time Out and Limitation on Connection Time

7.5.5.1 Systems sessions that are not active for more than 30 minutes are recommended to be automatically terminated where technically feasible. For those systems that cannot automatically terminate connections, password protected screen savers or terminal locks shall be activated.

7.5.5.2 PCs/laptops and Servers, when applicable, shall be configured with an approved password protected screen-saver in accordance to ***Section 7.3.2.1***

7.6 Application access control

Objective: *To prevent unauthorized access to information held in information systems.*

7.6.1 Information Access Restriction

7.6.1.1 All users shall only be provided with the minimum level of access required to perform their duties. The following can be considered:

- Logical security within an application
- Hiding the availability of unauthorized options
- Restricting access to command line driven navigation
- Restricting knowledge of application content and functionality
- Limiting file permissions, e.g. read-only
- Control of output distribution

7.6.2 Sensitive System Isolation

7.6.2.1 Application owners shall assess the need to run sensitive systems on stand alone computers.

7.6.2.2 Sensitive systems are recommended to be isolated in a dedicated computing environment.

7.6.2.3 When a sensitive application is to run in a shared environment, the application systems with which it will share resources should be identified and agreed with the owner of the sensitive application.

7.7 Monitoring system access and use

***Objective**: To detect unauthorized activities. Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents.*

7.7.1 Event Logging

7.7.1.1 All audit logs recording exceptions and other security-relevant events should be produced and maintained where possible. The following logs are relevant. (e.g. event logs) where technically feasible.

7.7.1.2 All security relevant events shall be logged on any computer or communications system handling confidential or executive information where technically feasible. This includes, but is not limited to, date and time of log-on and log-off, records of successful and rejected system access attempts, use of privileged accounts, records of successful and rejected data and other resource access attempts.

7.7.2 Monitoring System Use

7.7.2.1 Monitoring of all logs shall be allowed for authorized personnel only.

7.7.3 Clock synchronization

7.7.3.1 System clocks are recommended to be synchronized to ensure the accuracy of audit logs. For example, Greenwich Mean Time or Local time.

7.8 Mobile computing

***Objective**: To ensure information security when using mobile computing facilities. The protection required should be commensurate with the risks these specific ways of working cause.*

7.8.1 Mobile Computing

7.8.1.1 Mobile equipment includes personal handheld, notebooks and blackberry etc. shall be protected against unauthorized access.

7.8.1.2 Users are responsible to safeguard their mobile equipment and information stored in the mobile equipment.

7.8.1.3 Personal mobile computing equipment shall not be connected to the organization network without approval from Head of IT Department and department head by filling the ***IT-MOB-F001A - Employee mobile Form***

8. Systems Development and Maintenance

8.1 Security requirements of systems

Objective: *To ensure that security is built into information systems. This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.*

8.1.1 Security requirements analysis and specification

8.1.1.1 For all systems developed within or for BGC, security requirements shall be determined prior to the application development phase. During the system design phase, proper control environment of the application shall be determined.

8.2 Security in application systems

Objective: *To prevent loss, modification or misuse of user data in application systems. Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.*

8.2.1 Validation

8.2.1.1 Appropriate controls and audit trails or activity logs shall be designed into critical application systems. These shall include the validation of input data, internal processing and output data.

8.3 Cryptographic controls

Objective: *To protect the confidentiality, authenticity or integrity of information. Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.*

8.3.1 Policy on the use of Cryptographic Controls

8.3.1.1 Users shall not install any encryption software without prior permission from the IT Department.

8.3.1.2 Before cryptographic protections are implemented on a system, there shall be assessments on the risks and existing controls, which will help to determine the level of cryptography that may be needed, if needed at all. The IT Manager should be consulted on the potential need for encryption.

8.4 Security of system files

***Objective**: To ensure that IT projects and support activities are conducted in a secure manner. Access to system files should be controlled.*

8.4.1 Control of operational software

8.4.1.1 Master copies of all approved software shall be kept in a secure place.

8.4.1.2 All live applications and system software shall be secured from unauthorized amendment or deletion. The code is recommended to be version controlled and replaced only upon approval from the authorized personnel. An audit log of all updates to programs shall be maintained, and previous versions of software shall be retained.

8.4.1.3 All changes to operational software shall be evaluated prior to implementation on the live system to ensure the changes have no adverse impact on security or availability of systems. This includes development projects, version increments and bug fixes.

8.4.2 Protection of system test data

8.4.2.1 Where operational data is copied to a test system it shall be subject to a similar level of control as the live version. The controls shall include:

- Authorization
- Audit log maintained of activity and personnel

8.4.2.2 Live data can be requested in accordance to ***IT/SRT/PP001/Request for LIVE Data***.

8.4.3 Access control to program source library

8.4.3.1 All changes to the program source library shall be documented in software change procedures (***Section 8.5.1***).

8.4.3.2 Libraries/directories containing application source code shall be secured from unauthorized access using the following recommended controls where possible:

- Access controls to prevent IT staff gaining access to source code in an uncontrolled manner, and change control procedures implemented (Refer to ***IT/CMT/PP002/Software Application Change Management***)
- Separation of live source from development source libraries
- Authorization for updating program source libraries (Refer to ***IT/CMT/P002/Software Application Change Management***)

8.5 Security in development and support processes

Objective: *To maintain the security of application system software and information. Project and support environments should be strictly controlled.*

8.5.1 Change Control Procedures

8.5.1.1 All change request forms, program change test plans and testing results shall be documented and filed.

8.5.1.2 Testing procedures shall be properly documented in accordance to ***IT/CMT/PP002/Software Application Change Management.*** If problems are noted during the testing process, the developer will document the problem, make appropriate modifications in the development environment and submit it for retesting.

8.5.1.3 A formal review and sign-off on the application system changes shall be completed before live operation in accordance to ***IT/CMT/P002/Software Application Change Management.***

8.5.2 Technical Review of Operating System Changes

8.5.2.1 All operating system releases shall be checked for functionality and security. Implementations shall include back out planning. All operating system changes should follow ***IT/CMT/PP001/System and Network Change Management.***

8.5.3 Restriction on changes to software packages

8.5.3.1 Vendor-supplied software packages should be used without modification.

8.5.4 Outsourced Software Development

8.5.4.1 Outsourced development contract shall be agreed by business application owner(s).

8.5.4.2 When software development is outsourced, there shall be proper safeguard to manage such activities. The following should be considered.

- Licensing arrangements, code ownership and intellectual property rights
- Certification of the quality and accuracy of the work carried out
- Escrow arrangements in the event of failure of the third party, where possible
- Rights of access for audit of the quality and accuracy of work done
- Contractual requirements for quality of code
- Testing before installation to detect Trojan code

8.5.4.3 Software maintenance contract to specify escalation procedures for resolving persistent problems.

9. Disaster Recovery Planning

9.1 Aspects of disaster recovery planning

Objective: To counteract interruptions to business activities and to protect critical IT processes from the effects of major failures or disasters. A disaster recovery plan should respond to a disaster by recovering critical business functions within a defined time frame, thus minimizing loss and restoring affected areas efficiently.

9.1.1 Recovery and impact analysis

9.1.1.1 A risk assessment or strategy plan shall be determined to assist in the development and approach of disaster recovery planning. The risk assessment shall identify all key systems and critical business functions and the threats to those assets. The threats include, but are not limited to:

- Natural disasters
- Fire
- Loss of critical infrastructure services such as power, communications or water
- Deliberate or accidental damage to equipment or data
- System failures
- Security breaches

The likely impact of these threats shall be determined for each asset including a damage analysis and priorities for recovery including clearly defined recovery time objectives and minimum acceptable recovery resources.

9.1.2 Writing and implementing recovery plans

9.1.2.1 The Disaster recovery plan (DRP) shall restore or maintain business operations in the required time following any interruption of service or disaster. DRP shall be written in accordance to ***Boutique Group of Companies IT Disaster Recovery Plan.***

9.1.2.2 DRP shall have a designated owner of the plan and process. The responsibility of the disaster recovery owner includes maintenance and testing of the plan, development of execution criteria and requirements and determination of activation status.

9.1.2.3 The DRP shall be consistent with BGC standards, contain all necessary documentation, have approval by affected business units and meet all necessary requirements as determined by management.

9.1.2.4 The DRP shall have a testing schedule. Frequency of disaster recovery plan testing will depends on the criticality of the system as per assessment by the respective system owner in ***Boutique Group of Companies IT Disaster Recovery Plan***.

9.1.2.5 Staff should be trained on the agreed set of recovery procedures. Where possible, regular tests should be conducted to ensure staff knows how to react in response to the activation of disaster recovery.

9.1.2.6 The DRP is to be reviewed base on the determination of the DRP Owner.

10. Compliance

10.1 Compliance with legal requirements

Objective: *To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements*

10.1.1 Identification of applicable legislation

10.1.1.1 The design, operation, use and management of application systems shall compliant with statutory, regulatory and contractual security requirements.

10.1.2 Intellectual property rights (IPR)

10.1.2.1 All design, software, products developed shall be owned by BGC unless specified otherwise.

10.1.2.2 Copy of such software shall be made available to approved party only.

10.1.2.3 Staff shall not make a copy of it for personal use.

10.1.3 Software copyrights

10.1.3.1 Only licensed software shall be used for business activities within the organization. Software owners shall ensure that the software is used within the limits of the terms and conditions stated in the agreement

10.1.3.2 Staff shall not make unauthorized copies of the licensed software.

10.1.3.3 Software that is installed for trial run shall be removed from the system when the trial run period is over.

10.1.3.4 Records of software installed to-date should be maintained to ensure that the maximum number of licenses purchased has not exceeded. Original licenses and master copies shall be kept as evidence of ownership.

10.1.3.5 Original copy of the software shall be stored in a secured place centrally.

10.1.3.6 Staff who installs any unlicensed software shall be held fully responsible for any copyright infringement.

10.1.4 Prevention of misuse of information processing facilities

10.1.4.1 BGC information processing facilities such as computers are for business use only. The use of any BGC information processing facility for non-business purposes is strictly forbidden. Any activity shall be reported to management.

10.1.5 Collection of evidence

10.1.5.1 Process and system owners are recommended to ensure that the process and system design provides sufficient quality evidence when needed.

10.2 Reviews of security policy and technical compliance

Objective: *To ensure compliance of systems with organizational security policies and standards. The security of information systems should be regularly reviewed.*

10.2.1 Compliance with security policy

10.2.1.1 Management, Managers and staff are responsible for compliance of relevant sections of the BGC security policy.

10.3 System Audit Considerations

Objective: *To maximize the effectiveness of and to minimize interference to/from the system audit process. There should be controls to safeguard operational systems and audit tools during system audits.*

10.3.1 System audit controls

10.3.1.1 All audit activities shall be reviewed for proper audit planning and execution. This includes, but is not limited to:

- Minimizing any disruption or interruption of business operations
- Agreeing on all audit activities and objectives with management
- Limiting scope of assessment to a controlled environment ensuring no improper access is given to perform the audit tasks
- Identifying resource and skill needs for any technical tasks
- Logging all audit activities and providing documentation of tasks performed, audit procedures, findings and recommendations

10.3.2 Protection of system audit tools

10.3.2.1 Where applicable, all tools, including software, applications, documentations and work papers, required for system audits shall be protected from potential threats.