IT Operations and Network Security Policy

1. Purpose

1.1. Any loss, compromise, or misuse of Globespan Travel Management information and associated assets, however caused, could have potentially devastating consequences for Globespan Travel Management and may result in financial loss and legal action.

1.2. The purpose of this document is to define the policies and standards that will be applied to maintain the confidentiality, integrity and availability of the information systems supporting the business functions of Globespan Travel Management.

1.3. This policy provides management direction and support for the implementation of information security and is designed to help Globespan Travel Management employees carry out the business of Globespan Travel Management in a secure manner. By complying with this policy, the risks facing Globespan Travel Management are minimized.

2. Introduction

2.1. This policy applies to Globespan Travel Management employees, including temporary workers, independent consultants and contractors and suppliers/contractors responsible for managing and operating Globespan Travel Management information systems, computer and network facilities.

2.2. The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact Globespan Travel Management's IT Department.

2.3. The following policies should be read in conjunction with this policy:

- Information Security Policy Document
- Access Control Policy

- Acceptable Use Policy
- Information Handling and Protection Policy
- Physical and Environmental Security Policy
- Business Continuity Policy
- Code of Conduct for Globespan Travel Management Employees

3. Operational Procedures & Responsibilities

3.1. Procedures & Responsibilities Overview

3.1.1. The IT department will prepare appropriate documented operating procedures for all operational information systems, to ensure a correct and secure operation. Documented procedures are required for system development, maintenance and testing work, especially if it requires the support or attention of other organizational functions.

3.1.2. All operating procedures are formal documents and any changes are to be authorized by the process owner.

3.1.3. Documented procedures are prepared for:

- System housekeeping activities
- Network management
- Data back-up
- Change Control Management

3.1.4. Responsibilities and procedures for the management and secure operation of Globespan Travel Management resources and all connected PCs, laptops and networks are to be established. This is to include appropriate operating instructions and incident response procedures.

3.2. Change Management

3.2.1. Changes to equipment, software or procedures are subject to a formal change control process. The IT Department will ensure that all changes to the operational environment are:

- Assessed, where appropriate, for the potential impact of such changes
- Identified and recorded
- Formally approved
- Communication of change details to all relevant individuals
- Procedures and responsibilities for aborting and recovering from unsuccessful changes

3.2.2. Before installation on to the Globespan Travel Management network, all changes must be logged and authorized by the appropriate member(s) of staff.

3.2.3. On completion of any upgrade, modification or installation, the change control form must be updated to show all the work done and the version numbers of any software packages, patches or upgrades recorded.

3.3. **Incident Management**

3.3.1. Incident management and reporting responsibilities and procedures will be established to ensure a quick, efficient and orderly response to security incidents. (For examples of information security incidents, please refer to the *Acceptable Use Policy*.

3.3.2. Processes must be established to coordinate activities spanning Globespan Travel Management and all affected partners, and to determine how information will be disseminated to the public and media should this become necessary.

3.3.3. Once a security incident is reported, employees must immediately follow the incident response procedure. Senior Management must be clear on incident definitions and escalations for quick and appropriate response upon notification.

3.4. **Segregation of Duties**

3.4.1. Segregation of duties will assist in the prevention of fraud, errors, conflict of interest, minimize information security risks and reduce risk of accidental or malicious

system misuse.

3.4.2. Care is taken that no single individual can perpetrate fraud in areas of single responsibility without being detected. For example, the initiation of an event is separated from its authorization. The following points are considered:

- It is important to segregate activities that require collusion in order to defraud, e.g. the initiation and authorization of an event
- If there is danger of collusion, then controls need to be devised so that two or more individuals need to be involved, thereby lowering the possibility of conspiracy.

3.4.3. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision are considered.

3.4.4. Business need-to-know should be considered in conjunction with separation of duties to ensure that one does not override the other. Risk management and change management processes should include the discussion of separation of duties as well as business “need to know”.

3.4.5. No individual may approve his or her own changes. No individual should have unchecked control over an entire business transaction, infrastructure area, or environment.

3.4.6. Job roles and responsibilities should be reviewed to ensure there are no contradictions of responsibilities in this area.

3.5. **Monitoring System Access & Use**

3.5.1. Systems will be monitored to detect deviation from the *Access Control Policy* and record events to provide evidence in case of security incidents.

3.5.2. The application business owner must establish the logging and monitoring requirements for business auditing purposes. Designated employees responsible for the

following areas must establish the logging and monitoring requirements for the relevant purposes:

- Security
- Incident investigations
- Audit
- Fraud
- Legal

3.5.3. A process for capturing logging and monitoring requirements must be developed. Audit and event logs will need to be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties). Tools may be required for log analysis.

3.6. Reporting Security Weaknesses

3.6.1. It is vitally important that security events are reported. All security weaknesses must be reported immediately to the IT Department, who in turn will inform the VP Technology & Operations of associated risks, corrective or preventative actions.

3.6.2. Users should not, in any circumstances, attempt to prove a suspected weakness.

3.7. Reporting of Software Malfunction

3.7.1. Users of information processing services are required to note and report any software that appears not to be functioning correctly to the IT Department.

3.7.2. If it is suspected that the malfunction is due to a malicious piece of software (e.g. computer virus) the user is asked to:

- Note the symptoms and any messages appearing on the screen
- Stop using the equipment (isolate it if possible) and inform the service desk immediately.

3.7.3. If any investigations are to be performed on the equipment, it is disconnected from the network before being re-powered.

3.7.4. Users are informed that they should not, under any circumstances, attempt to remove the suspected software. Only trained and authorized employees may undertake recovery action.

3.8. Separation of Development, Test and Operational Facilities

3.8.1. The IT Department will ensure that development, test and operational systems are segregated (run on different processors or domains) in order to prevent unauthorized access, modification or misuse of information or services.

3.8.2. For each information or service, the need for separating development, production, test and operational facilities is determined through risk assessment.

3.8.3. The following levels of separation are considered and implemented, as appropriate, to mitigate any of the risks:

- Development and production software should, where possible, be run on different processors or in different domains or directories.
- Development and test work are separated as far as possible.
- Access to compilers, editors and other system utilities are separated from operational systems when not required.
- Different logon procedures are used for production and testing systems, to reduce the risk of confusion or error. Users are encouraged to use different passwords for these systems, and menus should display appropriate identification messages.
- Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.
- Live data that contains personal information must not be used for testing without being depersonalized before installation. All use of live data must be authorized by the information owner. Live personal data may not be used in training environments.

3.8.4. All domains/environments must be appropriately protected. Additional technology, both hardware and software, will be required to duplicate the development environment.

3.9. Capacity Management

3.9.1. The hard drive capacity of Globespan Travel Management's file servers will periodically be monitored by system administrators.

3.9.2. If free space on the file server hard drive becomes less than or equal to 20% of total capacity, users are requested to remove redundant files. If this is not possible, extra hard disk space should be installed.

3.9.3. Projections of future requirements should be made to prevent any bottlenecks and dependencies on the services by Globespan Travel Management or third party organizations.

3.10. **System Acceptance**

3.10.1. Acceptance criteria for new systems and system upgrades are to be established by the system owner and appropriate managers and suitable tests carried out prior to acceptance. This must include appropriate testing of security mechanisms. This will ensure that requirements for new systems are clearly defined, documented and tested.

3.10.2. The IT General Manager must ensure the evaluation and Risk Assessment has been applied and must ensure the correct management of system network provisioning, and hard and software deployment.

3.10.3. Adequate capacity and fallback planning must be carried out to ensure the availability of Globespan Travel Management resources.

3.10.4. Before installation, the system/upgrade must be appropriately tested to ensure no conflicts or vulnerabilities are introduced to the current Globespan Travel Management network.

3.10.5. All new systems/upgrades are to be controlled by the Change Control process. No systems/upgrades are to be implemented without due approval.

3.10.6. For major new developments, the operations function is consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests are carried out to confirm that all acceptance criteria are fully satisfied.

3.11. Protection from Malicious Software

3.11.1. The IT Department will deploy appropriate controls to mitigate the risks of viruses and malicious software. A process to update the controls must be in place.

3.11.2. Globespan Travel Management file servers, PCs and laptops will have antivirus software installed. The software is to be configured to scan all files for viruses. The software should automatically check for updates on a daily basis.

3.11.3. The IT General Manager will confirm and document that the latest update has been installed.

3.11.4. Employees must be educated on the use of these controls and made aware of the types of malicious code and the threats that they impose.

3.12. Mobile Code

3.12.1. Mobile Code is used on the Internet to run animation effects. Examples are 'Active X' or 'Flash Media'. If it is installed on Globespan Travel Management PCs it can cause damage to the network.

3.12.2. Mobile code must be authorized by the IT General Manager and kept isolated from any production environment. The use of such code must be restricted to authorized staff only.

3.12.3. Where mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy. Unauthorized mobile code should be prevented from executing.

3.13. Vulnerability Management

3.13.1. All exploitable vulnerabilities must be managed. The IT Department will ensure it has defined processes to identify vulnerabilities, prioritizing and mitigating all found. This will include specific patch application periods and a process for auditing compliance.

3.13.2. At minimum, this will include patching vulnerabilities being actively exploited immediately, critical vulnerabilities within 14 days, high vulnerabilities within 30 days and others within 60 days.

3.13.3. Regular network scanning of all devices for vulnerabilities must be carried out, at minimum a full network scan every 60 days.

3.14. **Information Back-Up**

3.14.1. The IT Department will ensure that adequate back up facilities of the Globespan Travel Management's internal systems are provided to ensure that all essential business information and software can be recovered following a computer disaster or media failure:

- A minimum level of back up information (together with accurate and complete records of the backup copies and documented restoration procedures) is stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations of cycles of backup are retained for important business applications.
- Back-up copies of essential business data, software and log files are to be taken at a frequency determined by the business owner, auditors and IT General Manager as appropriate. Back-up arrangements are to meet the requirements of business continuity plans.
- Back-up data is given an appropriate level of physical and environmental protection, consistent with the standards applied to the main site. Back-up data is to be regularly tested to ensure its viability for recovery when required.
- Back up information systems are regularly tested to ensure that they can be relied upon for emergency use when necessary.
- Restoration procedures are regularly checked and tested to ensure they are effective and can be completed within the time allotted in the operational procedures for recovery.

3.15. **Access Control**

3.15.1. Access to information and business processes will be controlled on the basis of business and security requirements.

3.15.2. An access management process for every system/database must be created, documented, approved, enforced and communicated to all relevant employees and partner organizations.

3.15.3. Each business application run by, or on behalf of Globespan Travel Management, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

3.15.4. Access to information must be based on "need to know" and segregation of duties. The appropriate information, system, database, or application owner is the only individual that can authorize a systems administrator to grant or update access via the formal access management process.

3.15.5. Audit must monitor the process to ensure that access control is appropriately implemented according to 'business need to know' and 'segregation of duty' principles.

3.15.6. Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

3.15.7. Access control requirements are clearly defined, documented and maintained within an Access Policy Matrix, which specifies the rights of individuals or groups of users. Globespan Travel Management has adopted common Windows-based operating systems, and predefined user profiles will be maintained to restrict access.

3.15.8. Screen savers or equivalent tools must be installed and enabled as part of a Standard Operating Environment (SOE).

3.15.9. All network equipment (including WAN service termination equipment, routers, hubs, cabling patch panels) will be kept in appropriate locked facilities. All network equipment outside computer rooms must be kept securely. Staff must ensure that doors are secured when they are left unattended. All equipment keys must be limited to staff who need them to carry out their duties. If any key is lost or mislaid, or any door found unlocked, then this must be reported immediately as an IT security incident.

3.15.10. All servers must be kept physically secure in an area for authorized individuals only. A process of allocating and monitoring access to server rooms must be implemented.

3.15.11.. For further information for employees, see the Globespan Travel Management's *Acceptable Use Policy*

3.16. **Controls on Data in Transit**

3.16.1. Information will need to be classified in terms of sensitivity and confidentiality. Information must be protected according to its classification and the minimum classification of the network it traverses.

3.17. **New & Obsolete Devices**

3.17.1 The infrastructure environment must be closely controlled and documented to minimize the introduction of unknown vulnerabilities.

3.17.2. The connection of new devices to Globespan Travel Management or partner connected infrastructure that might impact on the delivery of services must be requested and submitted for approval to the appropriate manager. Upon approval relevant documentation must be updated and submitted to the designated manager.

3.17.3. Similarly, disconnection of obsolete devices that might impact on the delivery of services must be requested and submitted for approval to the appropriate manager.

3.17.4. A configuration management process must be implemented and enforced.

3.18. **Detecting Unauthorized Changes**

3.18.1. The IT environment must be monitored to minimize the introduction of unknown vulnerabilities.

3.18.2. The IT General Manager will ensure that any new unauthorized device added to the network or device removed from the network without authorization will be detected, logged and the appropriate action taken. A configuration management process must be established.

3.19. **Media Handling and Security**

3.19.1. In order to prevent damage to assets and interruption to business activities, appropriate operating procedures will be established to protect information, documents, computer media, input/output data and system documentation. Appropriate controls need to be established for media handling and security.

3.19.2. Hard drives that contain ‘highly restricted’ information that are reused or require

replacement are securely erased or physically destroyed. If using the services of a third party for the management of media, a certificate is obtained as proof of destruction.

3.19.3. Software to securely erase hard drives will be considered and where possible configured to overwrite the media at least seven times.

3.19.4. A record is maintained of all removable media, e.g. backup tapes, to prevent any opportunity for loss or theft.

3.20. Exchanges of Information and Software

3.20.1. Exchanges of information and software between organizations will be controlled and compliant with relevant legislation, information sharing protocol(s), and handling requirements detailed in the appropriate risk assessment.

3.21. Security of System Documentation

3.21.1. Manuals, configuration details and network drawings are to be stored securely. Access to this documentation is only permissible by authorized employees. Copies of system documentation are stored off site. Access is limited to employees who are system administrators, i.e. staff with administrator privileges and the IT manager.

3.22. Mobile Computing and Teleworking

3.22.1. When using mobile computing or teleworking the risks of working in an unprotected environment are to be considered and appropriate protection applied.

3.22.2. Managers must be satisfied that an alternative work site (such as a home office) is appropriate for the tasks that are to be performed by the involved employee's member.

3.23.3. Supporting Material:

- Acceptable Use Policy
- Bring Your Own Device Policy
- Information Classification and Handling Policy

4. Network Access Control

4.1 Network Access Control Overview

4.1.1. Access to both internal and external networked services should be controlled to ensure that employees who have access to networks and network services do not compromise the security of these network services.

4.1.2 It must be ensured that:

- There should be appropriate interfaces between Globespan Travel Management's network and networks owned by other organizations or public networks.
- All users and equipment on the network are authorized, uniquely identified and authenticated
- User access to information services is monitored. Enforced path to limit routing capabilities will need to be considered.

4.2 Policy on Use of Network Services

4.2.1. The IT Department will undertake the following activities to control the use of its network.

- A risk assessment is undertaken for all connections to and from Globespan Travel Management networks, which is reviewed by the IT General Manager to ensure the process followed is adequate and comprehensive
- All connections to external networks must pass through a firewall or other appropriate network security device approved by the IT Department
- Modems and other external network connections e.g. VPNs may not be connected directly to the Globespan Travel Management network unless requested by Senior Management and approved by the IT General Manager.
- Modems with auto answer are not permitted
- Globespan Travel Management employees will be granted access rights to external networks only where there is a clear business requirement
- Access to external networks and systems must be authorized by a manager and used for business purposes only
- Access rights are revoked when access is no longer required

- The relevant system administrator or data owner will maintain a list of all access rules (Access Control Matrix) that will be approved by the senior management team
- Only authorized IT staff will be allowed to access diagnostic and configuration ports within Globespan Travel Management. All diagnostic ports not required are disabled.
- Globespan Travel Management will separate access to its network in accordance with the Access Policy Matrix
- Access control requirements are clearly defined and documented within Globespan Travel Management's Access Control Policy, which specifies the rights of individuals or groups of users to Globespan Travel Management's network.
- Globespan Travel Management should ensure that appropriate routing controls are implemented in accordance with the Access Control Policy and are based on source and destination address.

4.3. **User Authentication for External Connections**

4.3.1. Remote access rights to Globespan Travel Management systems are generally granted except where data processed is under third party agreements that forbid such access. Access for third parties is covered by the Third Party Security Policy.

- All remote access to Globespan Travel Management systems is authenticated by user account/password and where needed a second authentication factor.
- Access is subject to the same logical access controls as normal system access
- All communication will be encrypted

4.4. **Equipment Identification in Networks**

4.4.1. Automatic equipment identification is used as a means to authenticate connections from specific locations and equipment. All equipment will be identified using appropriate methods, and validated for compliance with policy before connection is permitted.

4.5. **Operating System Access & Control**

4.5.1. Security facilities at the operating system level will be used to restrict access to computer resources. These facilities are to be capable of the following:

- Identifying and verifying the identity, and if necessary the terminal or location of employees

- Recording successful and failed system accesses
- Providing appropriate means for authentication - if a password management system is used, it should ensure quality passwords
- Where appropriate, restricting the connection times of employees.
- Automatic terminal identification to authenticate connection to specific locations may be required. Terminal login procedures must be implemented. Use of system utilities may need to be restricted and tightly controlled.

4.6. **Security in Applications and Access Control**

4.6.1. Logical access to software and information should be restricted to authorized employees.

4.6.2. When designing an application system, security requirements, including appropriate controls and audit trails or activity logs, must be considered from the beginning of the project. The security requirements must balance the cost of implementation and the associated risks to the business.

4.6.3. Applications will:

- Control user access to information and application system functions
- Provide protection from unauthorized access
- Not compromise the security of other systems with which information resources are shared
- Be able to provide access to information only to the owner, other nominated authorized individuals, or defined groups of employees

4.7. **Systems Development & Maintenance Policy**

4.7.1. Security is an integral component of any systems acquisition, development and maintenance and applies to all aspects of systems development and maintenance whether performed directly by or on behalf of Globespan Travel Management.

4.7.2. The method for articulating security requirements is to be based on the agreed requirements and will be used as input to the design and implementation of the service and any subsequent accreditation.

4.8. **Security Requirements of Systems**

4.8.1. Security requirements should be identified and agreed prior to the development of information systems and aligned to the perceived threats and the value of the assets.

4.8.2. All security requirements, including the need for back-up arrangements, will be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

4.8.3. Considering security requirements from the beginning of a project minimizes costs since rework can be avoided as well as non-safe projects.

4.8.4. A process must be in place for reviewing the information security risk in all development projects.

4.8.5. The IT General Manager must be aware of all IT projects and their information security implications in order to provide recommendations and approval. It is the project manager's responsibility to obtain the IT Manager's approval prior to commencing each project phase such as proposal, design, release to production and maintenance.

4.8.6. Additional time and resources will be required in the project to incorporate information security risk assessment. Information security must be part of the formal application development methodology.

4.9. **Approving Information Security in Projects**

4.9.1. Information security requirements in terms of confidentiality, integrity and availability must be considered during the proposal, design, and release to production and maintenance phases for all projects, including acquisition of third-party software. The project manager must obtain approval for each phase from the IT General Manager.

4.9.2. The IT General Manager must be involved in all new or changed uses of information.

4.10. **Cryptographic Controls**

4.10.1. Cryptographic systems and techniques will be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

4.10.2. When evaluating the need for encryption, costs must be measured against the business risk. Particular attention should be paid to information held on portable devices.

4.11. Security of System Files

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

4.11.2. There must be controls for the implementation of operational software.

4.11.3. Controls may need to be applied around system test data. Access to confidential or restricted data stored in a shared system file must be commensurate with the classification of that data.

4.12 Security in Development and Support Processes

4.12.1 Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Lack of management and procedures to control changes to equipment, software or procedures can compromise operations.

4.12.2. Development and support environments will be strictly controlled to maintain the security of applications, system software and information.

4.12.3. Change management and configuration management processes must be defined that include procedures and responsibilities for aborting or recovering from unsuccessful changes.

4.13. Change Control Procedures

4.13.1. The formal change management process is to be followed for all operational changes to systems, equipment, software, standards, configuration or Processes/Procedures.

4.14. Audit Logging

4.14.1. Within each information system, appropriate audit logging must be implemented. The application business owner must establish the logging and monitoring requirements. Auditing should be configured to be operational at all times and sufficient information recorded to enable a thorough review of any suspected incident to be completed. The following events may be considered for audit as appropriate:

- User IDs
- Dates, times and details of key events, e.g. log-on and log off
- Terminal identity or location if possible
- Records of successful and rejected system access attempts
- Records of successful and rejected data and other resource access attempts
- Changes to system configuration
- Use of privileges
- Use of system utilities and applications
- Files accessed and the kind of access
- Network addresses and protocols
- Alarms raised by the access control system
- Activation and deactivation of protection systems, such as antivirus systems and intrusion detection systems

4.15. **Monitoring System Use**

4.15.1. The system administrator is responsible for monitoring access periodically or if a security breach has been detected or is suspected. Access to events logs will be restricted to security administrators. Events logs will monitor all system events, long on and log times and include:

- Authorized access:
  - user ID
  - date and time of event
- Privileged operations:
  - user of Administrator
  - root accounts
  - system startup and stop
  - all changes to privileges and user rights
- Unauthorized access:

- Unauthorized attempts to access information and information systems
- Unauthorized attempts to system commands

4.15.2. For each audited event, the Audit Log Record will contain at least the following:

- Date, time and nature of event
- User, process or PC ID (the user ID and the physical identifier of the PC involved will be used to assist in the investigation of any specific security related incident)
- Success or failure of the event
- Identity of the object being accessed (e.g. sufficient information is recorded to uniquely identify which database records are affected)

4.15.3. System access controls must be set to ensure that only the IT support staff have read access to audit logs and only system administrators have delete/archive access to audit information.

4.16. **Administrator and Operator Logs**

4.16.1. The IT General Manager and computer operators should maintain a log of all work carried out. Operator logs should include, as appropriate:

- Systems start and finish
- System errors and corrective action taken
- Confirmation of the corrective action taken
- The name of the person making the log entry

4.16.2. Operator logs are subject to regular, independent checks against operating procedures. All audit logs in support of the information security quality management should be retained for a minimum of six months.

4.17. **Environmental Monitoring**

4.17.1. Information processing facilities environments are monitored where necessary. Temperature, humidity and power supply quality is monitored where necessary to identify conditions that might adversely affect the correct operation of information processing equipment. These procedures are carried out in accordance with the manufacturers'

recommendations.

4.18.2. Refer to the *Physical and Environmental Security Policy*

4.18. Compliance

4.18.1. Globespan Travel Management expects that all employees will achieve compliance with this policy. This policy will be included within the internal audit information security programme, and compliance checks will take place to review the effectiveness of its implementation.

4.19. Exceptions

4.19.1. In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to a member of staff
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises

4.19.2. In such cases, the staff member concerned must take the following action:

- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non- conformance report
- Ensure that the situation is reported to the IT General Manager as soon as possible.
- Failure to take these steps may result in disciplinary action.

4.19.3. In addition, the IT General Manager maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified

- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

4.19.3. Globespan Travel Management will not take disciplinary action in relation to known, authorized exceptions to the information security management system.

4.20. **Penalties**

4.20.1. Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorized disclosure or viewing of confidential data or information belonging to Globespan Travel Management or partner organization
- Unauthorized changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of Globespan Travel Management or partner organization to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information security officer or senior management.

4.20.2. Any violation or non-compliance with this policy may be treated as serious misconduct.

4.20.3. Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

Review and update of this document will take place when changes require revising the **IT Operations and Network Security Policy**. Such modifications may relate to changes in roles and responsibilities, release of new legislation or the identification of a new policy area, in consultation with appropriate members and their approval on all revisions to this IT Operations and Network Security Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.

Document Configuration Control

Version No	Page No	Details of Change	Change Date	Prepared By	Approved By
1	All			Scott Duncan	Peter Lacy
1.1	All	Review	06 Aug 2020	Scott Duncan	Peter Lacy
1.2	All	Review	01 Oct 2020	Scott Duncan	Peter Lacy