include items such as specific training and testing requirements. A copy of the Risk Assessment, including the recommendation, will be sent to the manager requesting change.

The manager requesting change shall:

- Check the risk assessment and recommendation carefully to make sure that nothing has been missed.
- Notify the Business Information Systems Head of any missing risks or if there are problems with the recommendation.
- Authorize the risk assessment and recommendation.

9.5.6 The Implementation Plan

The Implementation Plan details all the stages that are required to successfully manage the change and includes a Test Plan and Roll Back Strategy. In more complicated changes this may also include a project schedule and timeline. The Project Manager shall draw up the implementation plan. The Head BIS requesting the change shall:

- Review the Implementation Plan.
- Make the Business Information Systems Head aware of any amendments or changes.
- Make note of the timeline and any training or testing and how this will affect department staff.
- Make note of any dependent tasks (i.e. if one department is unable to make a change until another has completed theirs).
- Authorize the Implementation plan.

9.5.7 Pre-Change

Once the Implementation Plan has been approved it is vital that the staff in each department is made aware of what needs to happen, when and by whom.

The Manager requesting change shall:

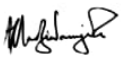
- Notify affected staff of the change and assign actions and make them aware of the roll back strategy.
- Ensure that staff who have been allocated test actions have copies of the test plan and are aware that all test documentation is to be retained.

TITLE: BUSINESS INFORMATION SYSTEMS PROCEDURE

This procedure is a mandatory element of the RTG ISMS and BCMS. There must be no deviation from this procedure but suggestions for improving the System should be discussed with the ISMS and BCMS Team for possible inclusion as amendments.

Approved: **Date: 02 October 2023**

Finance Director



Authorized: **Date: 02 October 2023**

Chief Executive

to the head of departments in the first instance and, where necessary, to the Business Systems Analyst. The policy and standards can be found on the RTG Limited Intranet.

1.5 RESPONSIBILITIES

a. Associates

- Make sure that information shared with colleagues, customers, contracted third parties and business partners is adequately protected proportionately to the risks involved
- Classify and clearly mark sensitive information
- Protect your workstation and security credentials (including user Ids, passwords and computer security tokens) against loss or compromise
- Never obtain, store or distribute any material which is illegal or likely to offend.
- Exercise care when using personal (including portable) computers and mobile phones, or when using email and internet access services
- Protect sensitive information that needs to be sent electronically, e.g. via email or transmitted over the Internet
- Never compromise sensitive information when using it in a public place, such as face-to-face conversations, mobile telephone calls, or the use of laptops on public transport.
- Comply with all laws and regulations governing issues such as data protection, software copyright, and computer misuse in the manner required by the company.
- Report any breaches or suspected breaches of this policy as well as weakness in Information security controls to your Head of Department.
- Report to General Manager about any unusual or unsolicited approaches from anyone trying to gain access to the information or the IT systems you have access to.

b. General Managers

- Ensure that there is an appropriate framework in place so that all staff comply with the policy and have the necessary skills, knowledge and awareness to do so
- Ensure that all staff are made aware of and apply the limits of their authority when using information and IT systems.
- Authorise, within their limits of authority, and periodically review, all access by staff to IT systems, physical buildings, and secure areas.
- Inform, in line with applicable laws and regulations, all staff of any IT Systems and/or buildings access that are being monitored
- Undertake and document an assessment of the risks arising from any non-compliance with the policy for your area of responsibility and ensure that the associated risks are being managed.
- Deal with any breach of policy by staff in accordance with policy procedures.
- Document, maintain and communicate any special local security arrangements necessary for the staff, IT systems and buildings that are under your management
- In addition to the above, managers of business areas that develop (or on behalf of which third parties develop) IT systems and services have a responsibility to ensure that risk assessments are performed at the appropriate project checkpoints for all

VERSION MANAGEMENT

Version management

Version	Date	Author	Nature of amendment
1.0	2 October 2023	BIS Committee	From Version 3 to Version 1.0 since BIS is removed from QMS scope to BSMS scope.

Table 1. Version history

POLICY: INFORMATION SYSTEMS POLICY	POLICY No: 1
RESPONSIBILITY: ALL RTG ASSOCIATES	EFFECTIVE DATE: 02 October 2023

1.0 INTRODUCTION

It is the policy of RTG Limited to protect all of the information it uses when conducting business, in accordance with its value and the risks to which it is exposed. This applies to all information, whether in written, spoken or electronic form. All staff must understand and discharge their responsibilities when using this information.

The BIS Policy is designed to ensure that in a continually changing business environment, we address a broad range of risks to our corporate and customer information. Information security concerns the protection of information and information systems from malicious or accidental loss, damage or abuse. The BIS Policy provides a framework for the protection of RTG Limited information and associated IT systems, whether internally or externally sourced. Implementation of this framework will also enable RTG Limited to meet its regulatory and legal requirements in all the jurisdictions in which it operates.

1.1 PRINCIPLES

The BIS Policy is underpinned by a set of Information protection principles:

- Information remains confidential where and when necessary
- Information can be relied upon for completeness and accuracy
- Information is available whenever the business needs it
- Transactions between RTG Limited and other parties cannot be falsely asserted or repudiated
- Information is used, maintained, stored and disposed of having properly considered all applicable laws, regulations, and contractual obligations
- Access to information and associated IT systems is accounted to an individual and restricted to the purposes associated with their role.

1.2 SCOPE

The policy applies to all staff within RTG Limited and they must establish executive ownership for the protection of information.

1.3 ADHERENCE

Adherence to the policy is mandatory. It is the responsibility of the General Manager to make appropriate provision for establishing controls to ensure adherence to the policy. Any breaches of policy will be dealt with in line with the organization's disciplinary procedures.

1.4 GOVERNANCE

It is owned by the Head – Business Information Systems and maintained by the BIS Department. All queries relating to policy implementation or compliance should be directed

2.3.3 Passwords Must Not Be Reused.

Users must not construct passwords, which are identical or substantially similar to passwords that they had previously employed. On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous fixed passwords. The history file must be employed to prevent users from re-using fixed passwords. The history file must minimally contain the last four (4) passwords for each user-ID.

2.3.4 Passwords Expiration.

Password expiration should be enforced on all accounts. The expiration period for user passwords should be set to 90 days (12 weeks) or less, after which the user should be forced to change the password before any other work can be performed.

2.3.5 Consecutive Unsuccessful Login Attempts

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts, the account must be locked for at-least one hour it is reset by a system administrator.

2.3.6 Difficult – To – Guess Passwords.

All user-chosen passwords for computers and networks must be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, vehicle license plate, PPS or social security number and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms and slang must not be employed.

2.3.7 Cyclical Passwords.

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters that change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

2.3.8 System-Generated Passwords.

If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other frequently changing unpredictable source.

new IT system and service developments and for significant changes to existing IT systems and services Document and communicate to the appropriate Information.

- In addition to the responsibilities of all General Managers, General Managers of business areas that operate (or on behalf of which third parties operate) IT systems or services have a responsibility to:
  - Ensure that all operational IT systems or services have a nominated owner to which key operational issues and risks can be escalated for resolution.
  - Ensure that risks to IT systems and services are managed in accordance with the requirements of the business area

c. Information Security Officer

- Enforce and verify compliance to the BIS Policy.
- Monitor levels of information security awareness and implement improvements where required.
- Develop, disseminate and maintain the ICT policies in line with the hanging threat, legislative and regulatory environments.
- Provide assurance to the executive management that the policy is effectively implemented across the organization
- Monitor and, where appropriate, lead the management and resolution of serious information security incidents
- Support the business by raising awareness of the requirements of the policy and providing advice and guidance on its interpretation within the individual business context

POLICY: PASSWORD POLICY	POLICY No: 2
RESPONSIBILITY: ALL RTG ASSOCIATES	EFFECTIVE DATE: 02 October 2023

2.0 INTRODUCTION

This Policy has been compiled to define the base level Password requirements for use within RTG Limited. The policy demonstrates RTG Limited's commitment to information security and its proactive approach to addressing risks within the organization.
One of the vital objectives of the BIS Department to operate a secure and controlled information systems environment is the deployment of approved security mechanisms that support its security services (identification, authentication, access control, data integrity and confidentiality). One of the key mechanisms is the definition and implementation of a uniform Password Policy throughout the organization. Any deviation from the Password Policy defined herein will require prior written approval of the Head of Business Information Systems (BIS).

2.1 SCOPE

The Password Policy applies to all accounts managed by the RTG Domain Controllers. The Password Requirements defined in this document apply to all systems that have the facilities to cater for them. Where systems do not have the facilities to cater for the Password Requirements, then alternative requirements, on a case-by-case basis, can be implemented with the prior approval of the Head of Business Information Systems.

2.2 OWNERSHIP & IMPLEMENTATION

Whereas this Password Policy document is owned by RTG Limited, it will be maintained by the Head of Business Information Systems in consultation with the Quality Department and other relevant areas within RTG Limited. The custodians of individual systems, servers, workstations, desktops and other devices are responsible for the enforcement of the Password Policy.

2.3 PASSWORD REQUIREMENTS

2.3.1 Minimum Password Length.

The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least eight (8) characters.

2.3.2 Password Complexity.

The password should contain a minimum of one (1) non-alphabetic character and should not contain more than two (2) consecutive repeated characters. The passwords must contain a mixture of upper and lower case characters and have at-least two (2) numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?":><|\).

2.3.9 Storage of System-Generated Passwords.

If passwords or Personal Identification Numbers (PINs) are generated by a computer system, they must always be issued immediately after they are generated. Regardless of the form they take, un-issued passwords and PINs must never be stored on the involved computer systems.

2.3.10 Assignment of Expired Passwords.

The initial passwords issued by an administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be performed.

2.3.11 Password-Based Boot Protection.

All workstations, no matter where they are located, must use an access control system approved by the BIS Department. In most cases, this will involve screensavers with fixed-password-based boot protection along with a time-out-after-no-activity feature.

2.3.12 Display and Printing of Passwords.

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. This includes, and is not limited to, passwords written on a piece of paper, where the paper might or might not be stored in a secure (under the keyboard, inside a drawer, in purse or wallet, etc.) location.

2.3.13 Protection of Passwords Sent Through the Mail.

If sent by regular mail, e-mail or similar physical distribution systems, passwords must be sent separately from user-IDs. These mailings must have no markings indicating the nature of the enclosure. Passwords must also be concealed inside an opaque envelope that will readily reveal tampering.

2.3.14 Encryption of Passwords.

Passwords must always be encrypted (non-clear text) when held in storage for any period of time (backup media, batch files, automatic log-in scripts, software macros, etc.) or when transmitted over networks. This will prevent them from being disclosed to wire tapers, technical staff who are reading systems logs, and other unauthorized parties. Passwords assigned by an administrator for a particular account (Initial account creation, or password resets for existing accounts) and systems used for account management are excluded from this specific requirement.

2.3.15 Prevention of Password Retrieval.

Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

2.3.16 Incorporation of Passwords into Software.

To allow passwords to be changed when needed, passwords should not be hard-coded (incorporated) into software developed or modified by RTG Limited Associates or third parties.

2.3.17 System Access Control with Individualized Passwords.

Computer and communication system access control must be achieved via passwords, which are unique to each individual user. Access control to files, databases, computers, and other system resources via shared passwords (also called lock words) is prohibited.

2.3.18 Passwords for each internal/external Network Device.

All RTG Limited network devices (routers, firewalls, access control servers, etc.) should have passwords or other access control mechanisms. A compromise in the security of one device will therefore not automatically lead to a compromise in other devices.

2.3.19 Changing Vendor Default Passwords.

All vendor-supplied default passwords must be changed before any computer or communications system is used for RTG Limited business operations.

2.3.20 Suspected Disclosure Forces Password Changes.

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. In the event passwords are found or discovered, the following steps must be taken.

1. Take control of the passwords and protect them.
2. Report the discovery to the BIS Helpdesk.
3. Transfer the passwords to the Business Information Systems Head.

2.3.21 Password Sharing Prohibition.

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for the actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, or other secure mechanisms as directed by the Business Information Systems Department.

2.3.22 Password for personal use only.

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like "guest").

2.3.23 Disclosure of incorrect log-in information.

When logging into RTG Limited computers, Servers or data communications systems, if any part of the log-in sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire login process was incorrect.

2.3.24 Un-attended systems or computing devices.

Systems and computing devices must not be left un-attended without enabling a password protected screensaver or lock screen or logging out of the device.

2.3.25 Disciplinary Actions.

Violation of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of RTG Limited Information Resources access privileges, civil, and criminal prosecution.

POLICY: DATA CLASSIFICATION POLICY	POLICY No: 3
RESPONSIBILITY: ALL RTG ASSOCIATES	EFFECTIVE DATE: 02 October 2023

3.0 PURPOSE

The policy is primarily concerned with the management of information to ensure that sensitive information is handled well with respect to the threat it poses to RTG Limited. Data classification helps us categorize data in a way that conveys the sensitivity of information, such as data that must be safeguarded for confidentiality, integrity, and availability.

Data is information in raw or unorganized form that refers to, or represent, conditions, ideas, or objects, it can be translated into a form that is more convenient to move or process. Data is a critical asset of the company. All associates have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the company, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form). Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of company data in compliance with this policy.

3.1 DATA CLASSIFICATION OUTSIDE EQUIPMENT

Data owned, used, created or maintained by the company is classified into the following three categories:

1. Public
2. Official
3. Confidential

3.1.1 Public Data

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to company disclosure rules, is available to all associates and to all individuals and entities external to the company.

- Press releases
- Notices
- Maps, newsletters, newspapers and magazines
- Published Accounts

3.1.2 Official Data

Official data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. Official data is information that is restricted to the company associates and departments who have a legitimate purpose for accessing such data.

- Departmental Information on associate computers and laptops.
- Data/Information stored on the company servers.

- Data/Information stored on other storage media stored offsite.

3.1.2.1 Handling Official Data

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Must not be posted on any public website.
- Must be destroyed when no longer needed; Hard Copy materials must be destroyed by shredding or
- Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the company's hardware and software policy

3.1.3 Confidential Data

Confidential Data is information protected by statutes, regulations, company policies or contractual language. Confidential data may be disclosed to individuals on a need-to-know basis only.

- Payroll data and information
- Associate related information
- Company performance data/information
- Data/information stored on the Corporate Office Management, Hotel Management and Directors and Directors computers and laptops.
- Data and information stored in
    - Windows 2008/2012/2016/2019 Server
    - Windows 7/8/10/11
    - Microsoft Project Server 2010/2013/2016/2019
    - Microsoft SharePoint server 2010/2013/2016/2019
    - Microsoft Office Professional 2010/2013/2016/2019
    - Microsoft Office Standard 2016
    - Office 365
    - Sophos End Point Protection
    - Veeam Backup Software
    - Micros POS 3700
    - Sage ERP Accpac Sage 300 cloud v2022
    - Opera PMS Version 5.6.15.0
    - VingCard
    - Midas / Man 3000
    - Linux
    - Open VPN
    - Materials Control Version 8.32.0.0
    - Belina Payroll

3.2 DATA OWNERSHIP

Data ownership formalizes the role of data owners and establishes accountability, assigning responsibility for managing data from creation to consumption. It puts rules and processes in place to ensure that the right people define usage directives, set quality standards, and consistently resolve data issues.

Table of data owners:

DATA	DATA OWNER
Windows 2012/2013/2016/2019 Server	BIS Department
Windows 7/8/10/11	BIS Department
Microsoft Project Server 2010/2013/2016/2019	BIS Department
Microsoft SharePoint server 2010/2013/2016/2019	BIS Department
Microsoft Office Professional 2010/2013/2016	BIS Department
Sophos End Point Protection	BIS Department
Sage ERP Accpac Sage 300 cloud v2022	Finance Department-Finance Manager
Opera PMS Version 5.6.15.0	Hotel Front Office Department-Front Office Manager
Belina Payroll	Human Resources Department-Payroll Manager
Materials Control	Hotel Food and Beverages Department-Food and Beverages Controller
Micros POS 3700	Hotel Food and Beverages Department-Food and Beverages Controller and Manager

3.2.1 Handling Confidential Data

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
- Must not be disclosed to parties without explicit executive management authorization.
- Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via email/fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Must be destroyed when no longer needed. Destruction may be accomplished by:

- "Hard Copy" materials must be destroyed by shredding after destruction, materials may be disposed of with normal waste.
- Electronic storage media shall be sanitized appropriately by degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the company hardware and software policy

The Business Information Systems Head must be notified in a timely manner if data classified as confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the company information systems has taken place or is suspected of taking place.

3.2.2 Data Retention

Data and Information shall be retained by the provision provided by the law. However, in the lack of such data shall be retained for the period of seven years.

POLICY: OPERA & MICROS PAYMENTS PROCESS FLOW	POLICY No: 4
RESPONSIBILITY: ALL CASHIERS	EFFECTIVE DATE: 02 October 2023

4.0 PURPOSE

This process flow comes as a result of the compelling objective to control, prioritize and optimally allocate cash resources and manage company-wide obligations thereby achieving operational efficiency. The license and support fees are controlled at central office. The BIS department is mandated to manage this aspect for the entire Group.

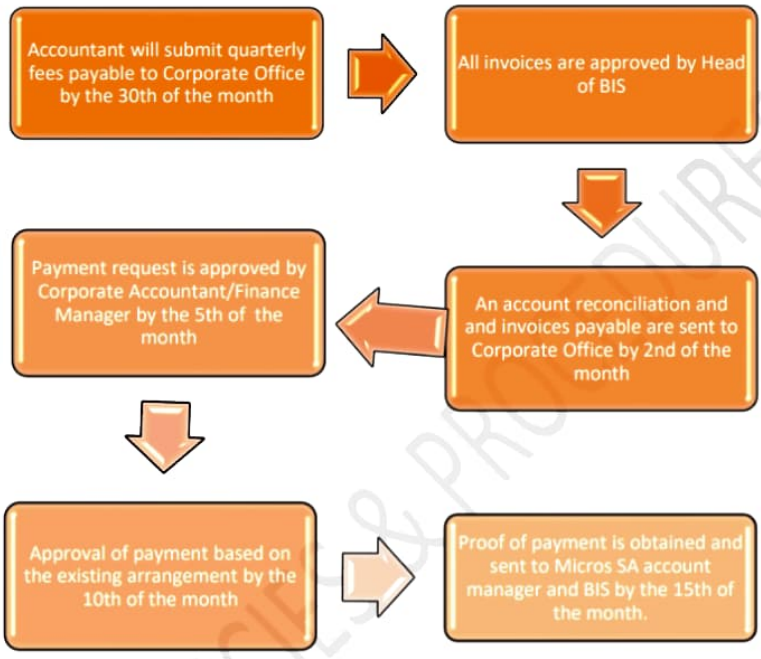
4.1 OBJECTIVES

a. Prioritization and efficient use of resources and across the business units.
b. Optimal allocation of resources and consistent procedure or process flow.

4.2 OPERATING PROCESS FLOW

1. Corporate office will receive quarterly support fees or service charges payable on or before the 30th of each month from units.
2. All invoices are approved by Head of BIS.
3. All unit accountants are expected to submit the account reconciliation and invoices to be paid by the 2nd of each month.
4. Approval of payment by Central Finance will be done by no later than the 5th of the month.
5. The payment will be raised by the 10th of the month through the RSA account. No other unauthorized payments will be tolerated.
6. Proof of payment (POP) is obtained from the bank by Accountant A 'Zambezi River Lodge who will forward it to the respective business unit accountant. The accountant will forward the POP to Micros SA account manager and copy to BIS by the 15th of the month.

4.3 Process Flow Summary



POLICY: SOCIAL MEDIA AND INTERNET ACCESS POLICY	POLICY No: 5
RESPONSIBILITY: ALL INTERESTED PARTIES	**EFFECTIVE DATE: 01 October 2023**

5.0 PURPOSE

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include Blogs, Wikis, Microblogs, Message Boards, Chat Rooms, Electronic Newsletters, Online Forums, Social Networking Sites, and other sites and services that permit users to share information with others in a contemporaneous manner. This covers RTG Limited hosted social media, and in non- RTG Limited social media in which the associates of RTG Limited affiliation is known, identified, or presumed.

5.1 SCOPE

The Scope of this policy applies to RTG Associates, Contractors, Volunteers or Members who facilitate the use of Social Media Technologies on behalf of RTG Limited. It also applies to an Associate's personal use of Social Media, when the Associate's or Contractor's affiliation with RTG Limited is identified, known, or presumed. It does not apply to content that is unrelated to RTG Limited.

The risks associated with Social Media use can be classified as Technological Threats and Content-Based Threats. The technological threats are the obvious risks such as malware distribution and infection. Content-Based risks include inappropriate distribution of intellectual property or offensive content, phishing, retention of business records and revelation of private or confidential information in a public setting. Content-Based threats are more difficult to prevent or detect using automated systems. Fundamentally, content-based threats are shared by all forms of human communication. Control of content-based threats is achieved by influencing the communications behavior of Associates across all platforms, not just social media. The IT security team can assist to a limited extent, but responsibility lies with the people and organizations in charge of corporate communications.

5.2 SOCIAL MEDIA

Social media is a form of Software as a Service (SaaS). The popular systems - such as Facebook, Twitter, Linked-In, Instagram to name just a few - are available from just about anywhere on the internet. This creates a serious problem for any organization that thinks blocking access from work will prevent security problems from social media. Associates can access social media from home or from a handheld device, after all. Blocking access at the work site prevents the corporation from observing and supervising associates use of social media, but it does not lessen the security risk. A number of solutions are available that enable the organization to provide controlled, filtered and monitored access to the most popular social media outlets (Facebook, LinkedIn and Twitter). These

solutions enable fine-tuned access control to social media features, filtering of content uploads and the capture and retention of business communications.
Security teams should also actively engage themselves in social media monitoring, analysis tools and services to discover information posted in public environments that relates to the security of the corporation. Associates must adhere to other IT related RTG Limited policies when using or participating on social media. All the rules that apply to other RTG Limited IT policies apply in social media communications.

5.3 PROCEDURES AND PRACTICES

The following principles apply to professional use of social media on behalf of RTG Limited as well as personal use of Social Media when referencing RTG Limited:

- Social Media use shouldn't interfere with employee's responsibilities at Rainbow Tourism Group Limited. RTG Limited's computer systems are to be used for business purposes only. When using RTG Limited's computer systems, use of social media for business purposes is allowed (e.g.: Facebook, Twitter, RTG Limited's blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Use the Social Media platforms after office hours if such use is for purposes other than duties assigned as expected by the associate's daily responsibilities.
- Subject to applicable law, after-hours online activity that violates RTG Limited's Code of Conduct or any other company policy may subject an Associate to disciplinary action or termination.
- If Associates publish content after-hours that involves work or subjects associated with RTG Limited, a disclaimer should be used, such as this:
  "The postings on this site are my own and may not represent RTG Limited's positions, strategies or opinions."
- Use Social Media sites to your advantage, for instance, before meeting with new clients or prospects, check their LinkedIn or other sites to obtain information that will help enhance the connection.
- Make sure Associate profiles are up to date, professional and relevant.
- Do not share your personal opinions about RTG Limited or your coworkers on social media sites.
- Do not blog or post anything about any financial, corporate or staffing information that is confidential, non-public or proprietary to RTG Limited or its clients or partners. This applies to personal and professional postings or commentary. It should be clear that not complying with this policy will invoke the appropriate disciplinary action by RTG Limited
- Do not blog about co-workers. Never put a co-worker's information or image on a Facebook page or other Social Media site without the approval of the Associate and/or the corporate affairs department.
- Do not blog or post anything to social media sites about a client, unless it is your specific job to do so. If it is your job, you must disclose who the clients are and the nature of the client business. Do not misrepresent a client or post anonymously.

- It is highly recommended that associates keep RTG Limited related social media accounts separate from personal accounts, if practical.
- Associates need to know and adhere to RTG Limited's Code of Conduct, Associates Handbook, and other company policies when using social media in reference to RTG Limited.
- Associates should be aware of the effect their actions may have on their images, as well as RTG Limited's image. The information that Associates post or publish may be public information for a long time.
- Associates should be aware that RTG Limited may observe content and information made available by associates through social media. Associates should use their best judgment in posting material that is neither inappropriate nor harmful to RTG Limited, its Associates, or customers.
- Although not an exclusive list, some specific examples of prohibited social media and online conduct include posting commentary, content, videos or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
- Associates are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, Associates should check with the Human Resources Department and/or their supervisor.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Associates should refer these inquiries to authorized RTG Limited spokespersons.
- If associates encounter a situation while using social media that threatens to become antagonistic, Associates should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Associates should get appropriate permission before you refer to or post images of current or former Associates, Members, Vendors, Contractors or Suppliers. Additionally, Associates should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Associates are further advised to refer to **HR029 Internet Usage Policy** for further information on using internet.

POLICY: EMAIL POLICY	POLICY No: 6
RESPONSIBILITY: ALL INTERESTED PARTIES	EFFECTIVE DATE: 02 October 2023

6.0 INTRODUCTION

Electronic mail system is any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system. This policy applies to all associates when using the electronic mail in RTG Limited and on behalf of RTG Limited. Every associate has a responsibility to maintain the company's image, to use the electronic mail system in a productive manner and to avoid placing the company at risk of legal liability based on their use. Misuse of email can lead to many legal, privacy and security risks, thus it is important for associates to understand the appropriate use of electronic communications.

6.1 PURPOSE

The purpose of this email policy is to ensure the proper use of email systems and make users aware of what is deemed as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within RTG Limited's Network and Email System.

6.2 SCOPE

This policy covers appropriate use of any email sent from an RTG Limited's email address and applies to all employees, vendors, and agents operating on behalf of.

6.3 USE OF ELECTRONIC MAIL

All messages distributed via the company's email system, even personal emails, are RTG Limited property. Associates must have no expectation of privacy in anything that is created, stored, sent or received on the company's email system. Emails can be monitored without prior notification if RTG Limited deems this necessary. If there is evidence that an associate is not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action, including termination and/or legal action.

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that associates are aware of the legal risks of email:

- An email message may go to persons other than the intended recipient. If it contains confidential or commercially sensitive information, this could be damaging to RTG Limited.
- Letters, files and other documents attached to emails that belong to others, by forwarding this information, without permission from the sender, to another recipient, this is liable to copyright infringement.
- When using the email system, take the opportunity to check for accuracy. If an email is sent with any libelous, defamatory, offensive, racist or obscene remarks, the associate and RTG Limited can be held liable.

- All RTG email must be scanned for viruses before sent, if you send an attachment that contains a virus an associate and RTG Limited can be held liable. By opening emails and attachments from an unknown sender an associate may introduce a virus into RTG Limited computer system generally.

6.4 RULES FOR EMAIL USE

RTG Limited considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Associates should take the same care in drafting an email as they would for any other communication. Therefore, adherence to the following rules is encouraged:

- It is strictly forbidden to use RTG Limited email system for anything other than legitimate business purposes. Therefore, the sending of personal emails, chain letters, junk mail, and jokes is prohibited. All messages distributed via the company's email system are RTG Limited property.
- All emails will carry a disclaimer stating that the email is intended only for RTG Limited use and if used for any other purpose a named person should be contacted immediately within RTG Limited.
- Particular care should be taken when sending confidential or commercially sensitive information. If in doubt, please consult the Business Information Systems Head.
- Great care must be taken when attaching documents or files to an email. Letters, files and other documents attached to emails may belong to others. By forwarding this information, without permission from the sender, to another recipient you may be liable for copyright infringement. Again, if in doubt, please consult the Business Information Systems Head.
- Sending email that is intimidating or harassing.
- Using email for purposes of political lobbying or campaigning.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of e-mail software such as bulk SMS relaying software.
- Do not send excessively large messages and attachments.

6.5 BEST PRACTICES

- All sensitive RTG Limited material transmitted over external network must be encrypted.
- All user activity on RTG Limited Information Resources assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of RTG Limited, or any unit of the RTG Limited unless appropriately authorized (explicitly or implicitly) to do so.
- Individuals must not send, forward or receive confidential or sensitive RTG Limited information through non-RTG Limited email accounts. Examples of non-RTG Ltd. email

accounts include, but are not limited to, Gmail, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

POLICY: SOFTWARE/HARDWARE POLICY	POLICY No: 7
RESPONSIBILITY: ALL BIS ASSOCIATES	EFFECTIVE DATE: 02 October 2023

7.0 PURPOSE

This Software and Hardware Policy defines the boundaries for the "acceptable use" of the company's electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the RTG Limited are to be used only for processing company-related materials. By using the RTG Limited hardware, software, and network systems the associate assumes personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies.

7.1 SOFTWARE

All software acquired for or on behalf RTG Limited or developed by company associates or contract personnel on behalf of RTG Limited is and shall be deemed company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. The associates or contract personnel shall sign device enrollment forms giving them access to usage and installation of the mentioned software.

7.1.1 Purchasing

All purchasing of company software shall be centralized. The BIS department shall assist the procurement department in ensuring that the software and hardware purchases are at the best possible price and required standards. All software and hardware Capex Expenditure forms shall include the section for the Business Information Systems Head signature.

7.1.2 Licensing

All software and hardware licensing requirements shall be done through the Business Information Systems Head. However, each associate is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on company computers and must notify the Business Information Systems Head for any breach or none-compliance.

7.1.3 Software Standards

The following list shows the suite of software in use by RTG Limited

- Windows 2008/2012/2016/2019 Server
- Windows 7/8/10/11
- Microsoft Project Server 2010/2013/2016/2019
- Microsoft SharePoint server 2010/2013/2016/2019
- Microsoft Office Professional 2010/2013/2016
- Microsoft Office Standard 2016
- Office 365
- Veeam

- Sophos End Point Protection
- Crash Plan Code42 Backup Software
- Micros POS 3700
- Sage ERP Accpac Sage 300 cloud v2022
- Opera PMS Version 5.6.15.0
- VingCard
- Midas / Man 3000
- Asterisk
- Linux
- Open VPN
- Materials Control Version 8.32.0.0
- Belina Payroll

Associates needing software other than those programs listed above must request such software from the information technology department. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

7.2 HARDWARE STANDARDS

All hardware devices acquired for or on behalf of the company or developed by company associates or contract personnel on behalf of the company is and shall be deemed company property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

7.2.1 Purchasing

All purchasing of company computer hardware devices shall be centralized with the information technology department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price. All requests for corporate computing hardware devices must be submitted to the General Manager for approval. The request must then be sent to the information technology department, which will then determine standard software that best accommodates the desired request. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements. The associates shall sign device enrollment forms giving them access to usage and software installation of the mentioned hardware.

7.2.2 Hardware Models

The following table shows the management levels and the hardware models applicable for use by members of staff on applicable to the management levels;

Management Level	Models
Executives	HP or Dell X 360 i7 or Higher
Corporate Office Senior Managers	HP Spectre i7 or Higher
Corporate Office Managers	HP ProBook i7, HP EliteBook i7
Corporate Office Staff	HP ProDesk 400 i7 or Dell desktop or higher

General Managers	HP Envy or Pavillion i7
Hotel Management	HP ProBook i7
Marketing Team	HP Mini i7 /MacBook i7
BIS Administrators	HP Probook i7, or higher
Accountants	HP Envy or ProBook i7, i9
Hotel Staff	HP ProDesk400 Desktop, Dell all in one, Dell desktop

7.2.3 Outside equipment

No outside equipment may be plugged into the company's network without the Business Information Systems Head's permission. The Business Information Systems Head can request the equipment to be scanned and certified by the IT department before use.

POLICY: NETWORK FIREWALL POLICY	POLICY No: 8
RESPONSIBILITY: ALL BIS ASSOCIATES	EFFECTIVE DATE: 02 October 2023

8.0 INTRODUCTION

A Firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules or policies. It is a security device used to stop or mitigate unauthorized access to a private network (in this case Rainbow Tourism Group internal network). Rainbow Tourism Group has since deployed and is currently being protected by Sophos XG perimeter Firewalls across its six Business Units.

8.1 PURPOSE

This firewall policy applies to and helps protect RTG Limited Information, assets availability, confidentiality, and integrity from outside intrusion and hacking. The firewall policy gives practical guidance in developing and implementing a standard RTG firewall policy.

8.2 SCOPE

The Scope of this policy applies to all Sophos XG perimeter firewalls currently deployed across the Rainbow Tourism Group Limited Business Units whether managed by RTG BIS personnel or third parties. Any changes or departure from this policy will be permitted only if approved by Head-Business Information Systems Manager or his/her designee. Any other devices configured to the roles of firewalls must be managed according to the rules defined in this policy.

8.3 GENERAL CONFIGURATION INFORMATION OF THE RTG FIREWALL POLICY:

The following policies and rules sets have been configured and applied to provide security guidelines or policy standards on all the RTG Sophos XG Firewalls.

a) Logical Access:

Logical access to all the Sophos XG Firewalls is available internally via the statically assigned LAN IP Addresses, SSL VPN, and via the Sophos Central Dashboard. The Sophos Central Dashboard is the cloud based unified console for other Sophos products in one place, that is XG Firewalls, Endpoint, Server with Intercept X, email, web. Sophos Administrator or BIS Network & Security personnel will have privileged super user rights for the purposes of day to day administration of the firewall devices. The Sophos Vendor will have logical access for the purposes of technical support which will only be activated if a fault is reported.

b) Inbound Real-time Internet Connections:

All inbound real-time internet connections to Rainbow Tourism Group internal network must pass through the Sophos XG firewall before users get access. All Rainbow Tourism Group computer systems will be protected by a firewall that is all servers, desktops, laptops, etc.

c) Inbound and Outbound Traffic:

All inbound and outbound traffic not expressly required will be blocked to reduce the risk of attack and decrease the volume of traffic traversing through the internal network. Configurations in this firewall policy will restrict all traffic, inbound and outbound from untrusted wired/wireless networks and hosts and specifically deny all other traffic except for necessary allowed protocols

d) Anti-Spoofing:

Anti-Spoofing measures will be applied to detect and block malicious source addresses from entering the internal network.

e) Default Firewall Passwords:

Default firewall passwords will be changed to further enhance device security and will be long enough to meet requirements defined by the password policy document.

f) Support and Maintenance:

All support and maintenance contracts of all Sophos Firewalls will be done through the approved Sophos Vendor and response times will be guaranteed as defined in the SLA.

g) Configuration Rules and Policies:

Configuration rules and policies shall be managed by a formal change request document. This means that all changes to the firewall software, upgrades and patches must go through the change request process.

h) Firewall Physical Security and Access:

All Rainbow Tourism Group firewalls must be located in a secured data center and only the RTG network and security personnel and Firewall approved vendors will be granted privileged access to the Sophos firewall.

i) Firewall Security Logs:

Firewall security logs will be configured, monitored periodically for anomalies. Changes to the firewall configuration parameters and enabled services must logged. All suspicious activity which could be an indication of unauthorized access or attempt to compromise security measures must also be logged.

j) Encrypted Web Connections:

SSL digital certificate will be configured to provide website authentication and encrypted connection to make sure that all websites connection by users are secure and legit.

k) Spam Filtering

Spam filtering protocols will be configured to restrict malicious traffic. Anti-spoofing measures will be implemented to detect and block unauthorized source addresses from entering the internal network

l) Firewall Licenses/Subscriptions:

Firewall licenses or subscriptions will be done/renewed as specified in the SLA through the authorized Firewall Vendor.

POLICY: CHANGE MANAGEMENT AND PROCEDURES POLICY	POLICY No: 9
RESPONSIBILITY: ALL RTG MANAGEMENT	EFFECTIVE DATE: 02 October 2023

9.0 PURPOSE

To define a Change as understood by the Company and describe the accepted Change Management procedure.

9.1 DEFINITION

Any change which may affect information transactions processing, management reporting and compliance. This includes the Control Environment (i.e. all systems business processes which may impact on the above). The key activities required are:

- Monitoring.
- Informing and communicating.
- Control activities (reviews and reports).
- Risk Assessments.
- Control environment (i.e. passwords, user access).'

In order to demonstrate that we have adequate control over our information systems we must also be able to demonstrate control over the wider operational environment.

9.2 SCOPE

This procedure is intended for all corporate and hotel management team members who have identified a change requirement. Only corporate and hotel management team members may request a change.

9.3 RISK

If not properly controlled changes could be made which negatively impact on the business and prevent people from fulfilling their roles. Changes could be made by individuals who are not fully aware of the impact on other areas of the business. If change is not controlled the Business could be exposed to fraudulent activities.

9.4 RESPONSIBILITIES

The corporate and hotel management team members ensure that changes follow the Change Management Procedure. The Business Information Systems Head reviews the Change Management Schedule monthly to ensure all changes follow the change management procedure.

The management committee reviews the change management schedule quarterly to ensure changes follow the change management procedure.

9.4.1 Roles

9.4.1.1 Business Information Systems Head/Business Systems Analysts

It is the Business Information Systems Head's role to facilitate communication between the Department requesting the change and any other affected Department. He/she co-ordinates all

of the documentation, acquisition of requirements, formulations of plans and scheduling of projects and tasks.

9.4.1.2 The Manager – Requestor of Change

It is the role of the requesting manager to review, comment on and authorize documents relating to the change, instruct staff and to participate in meetings to ensure that the change goes as smoothly as possible and that compliance is retained. His/her roles are:

- To understand the change management process and undertake the necessary training.
- As a change raiser he/she owns the change process and is responsible for the progression of the process from creation through to completion.
- To ensure that the change is raised as soon as a need for the change is known and there is sufficient detail to complete the change request form to the standards outlined.
- To communicate any service outage either as a result of the change or due to invocation of blackout to interested parties and, where appropriate, to obtain acceptance and agreement for the change to proceed.
- To ensure that the associated tasks are checked on time to allow the change to open for approval within the lead-times for that classification of change.
- For emergency changes, ensure that any associated Incidents or Problem records are correctly detailed within the 'Related Records' tab on the change record, and support the need for the fix change.
- It is the responsibility of the corporate and hotel management team to ensure that changes are approved by the appropriate areas prior to the implementation date.

9.4.1.3 The Change Implementation Team

The role of the change implementation team will be

1. To understand the change management process and undertake the necessary training.
2. To understand the overall change and how their specific task(s) contribute to the change.
3. To check or reject the task within the relevant time scale ensuring that:

- The task(s) assigned to their team contain accurate information to enable them to perform the task.
- The timescales within which to perform the work are achievable.
- The change will not inadvertently activate any other change already in the system.
- The change is only scheduled to activate at the approved time.
- Tasks are completed in the correct sequence.
- All pre and post implementation checks are performed as planned.
- In the event of back-out all post checks are performed to ensure services have been restored.
- To raise incidents when issues are encountered during implementation (failed and assisted changes)
- To ensure that adequately experienced support staff will be supporting the implementation.

- To ensure that the change poses no threat to the stability of the infrastructure/application and the configuration items being changed are correct
- To ensure that the change does not conflict with other planned activities on the same infrastructure

In all cases the team shall be made up of at least:

- PROJECT SPONSOR:- Manager requestor for change
- PROJECT MANAGER:- Business Information Systems Head/Business Systems Analyst
- Project Members

9.5 CHANGE PROCEDURE

9.5.1 Types of change

9.5.1.1 Minor Changes

A minor change is one which does not have a noticeable impact on the IT services provided to the departments.

Examples of minor changes are as follows:

- Active directory changes
- All system password changes
- Electronic email system configuration changes

9.5.1.2 Significant Changes

These are changes which are not likely to cause a service outage but has an impact to the services provided by the businesses if it is not done correctly.

Examples of significant changes are as follows:

- Opera rate changes.
- Micros menu changes
- Hardware installations
- Microsoft Software upgrades, patches, scripts and security updates
- Sage AccPac system configuration changes
- Belina Payroll system configuration changes

9.5.1.3 Major changes

A major change can be defined as a change with a potential risk of causing an outage, reducing service and affecting performance targets and can adversely affect users and IT systems users during core service hours. Examples of major changes are as follows:

- Change in business processes and procedures.
- Change initiated by the authorities e.g. Government, Insurance sector regulators
- Disconnection of mains power supply
- Core systems hardware installation & movements
- Network cable rerouting, installation or repair
- New release/version software installation
- Internet service provider servers outages

9.5.1.4 Outage Changes

These will cause interruption and stoppage to normal services, examples of outage changes are as follows:

- Change of critical systems;
  - Microsoft Servers Systems
  - Opera PMS
  - Micros POS
  - Materials Control
  - Sage Accpac ERP
- Relocation of Data Centers/Server Rooms.
- Change of BIS service providers especially for networks and critical systems
- Restructuring of the BIS department.

9.5.2 Submit the Change Request Form

1. Complete a Change Request Form.
2. Enter as much detail as possible in the Request Details section. If this change will affect other departments, please enter the names of the other departments affected section. If your change is urgent, please tick the Emergency Change Needed on the form.
3. Once the form has been completed, submit the form to the Business Information Systems Head.

9.5.3 Review the Specification

The Change request form will be reviewed by the Business Information Systems Head who will gather additional information, add any member of the corporate office or hotel management team deemed to be affected and arrange meetings. The Business Information Systems Head creates a specification detailing what is being changed. The Specification should incorporate all the requirements.

- The manager requesting change will carefully review the specification to ensure that all the requirements and their particular interests are covered.
- The manager will need to approve the specification.
- The Business Information Systems Head will discuss what the appropriate Change Rating should be with the manager and the department affected. In essence the Change Rating indicates the level of compliance required by the change and the priority that the change is being given.

9.5.4 The Project Plan

The Business Information Systems Head will draw up a project plan using the Microsoft Project, showing clearly the major project milestones and the project critical path. The project plan is submitted to the manager requesting change for review.

The manager requesting change shall;

- Check the project plan against project deliverables
- Notify the Business Information Systems Head for any project planning discrepancies.

9.5.5 The Risk Assessment

The Information Security Officer will conduct a risk assessment based on the agreed specification. He/she will check all the systems and processes affected by the proposed change and list any risk areas. The Risk Assessment is used to create a change recommendation to ensure that any risk to the business has been identified and mitigated. The recommendation will include items such as specific training and testing requirements. A copy of the Risk Assessment, including the recommendation, will be sent to the manager requesting change.

The manager requesting change shall:

- Check the risk assessment and recommendation carefully to make sure that nothing has been missed.
- Notify the Business Information Systems Head of any missing risks or if there are problems with the recommendation.
- Authorize the risk assessment and recommendation.

9.5.6 The Implementation Plan

The Implementation Plan details all the stages that are required to successfully manage the change and includes a Test Plan and Roll Back Strategy. In more complicated changes this may also include a project schedule and timeline. The Project Manager shall draw up the implementation plan. The Head BIS requesting the change shall:

- Review the Implementation Plan.
- Make the Business Information Systems Head aware of any amendments or changes.
- Make note of the timeline and any training or testing and how this will affect department staff.
- Make note of any dependent tasks (i.e. if one department is unable to make a change until another has completed theirs).
- Authorize the Implementation plan.

9.5.7 Pre-Change

Once the Implementation Plan has been approved it is vital that the staff in each department is made aware of what needs to happen, when and by whom.

The Manager requesting change shall:

- Notify affected staff of the change and assign actions and make them aware of the roll back strategy.
- Ensure that staff who have been allocated test actions have copies of the test plan and are aware that all test documentation is to be retained.

- Liaise with other departments and the Business Information Systems Head to ensure that all aspects of the change are progressing as planned.

9.5.8 Change

To minimize unnecessary disruption, ensure that the plan is followed as closely as possible and any issues are highlighted to the Business Information Systems Head as soon as possible. Who shall coordinate the communication between all the stakeholders and ensure all staff follow the implementation plan.

9.5.9 Post Implementation Review

- Once a change has been implemented it is important that the situation is reviewed to identify any problems that could be prevented in future or improvements that could be made.
- The Business Information Systems Head and the manager will carry out a Post Implementation review one month after the change has been promoted to Live (unless problems or issues present themselves more immediately). This can be done using the Post Implementation Review form.
- Two months after the change has been implemented the Business Information Systems Head and the manager will conduct a further review.
- The Management Committee which is made up of the RTG Limited Senior management will review change documentation and follow up material quarterly. The minutes and action points of these reviews are held on file with the change documentation by the Business Information Systems Head.
- The Internal and External Auditors will examine the change management documentation on a half yearly and End of Year basis and their comments and recommendations will be acted upon.

9.5.10 Change Request Form

This form is divided into three sections. **Section 1** is intended for use by the manager submitting the change request. **Section 2** is intended for use by the Business Information Systems Head to document/communicate their initial impact analysis of the requested change. **Section 3** is intended for use by the Management Committee to document their final decision regarding the requested change.

POLICY: REMOTE ACCESS POLICY	POLICY No: 10
RESPONSIBILITY: ALL INTERESTED PARTIES	EFFECTIVE DATE: 02 October 2023

10.0 INTRODUCTION

Today's computing environments often require out-of-office access to information resources. Remote access refers to the process of connecting to internal resources from an external source (home, hotel, district, or other public area). The ability to securely and reliably connect to business resources from a remote location increases productivity.

10.1 PURPOSE

This policy compliments the Access Policy, as both documents are necessary for implementing a safe Access policy for RTG Systems and Technology Resources. It provides guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the corporate network. The purpose of this policy is to define the rules and requirements for connecting to our organization's network from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

10.2 SCOPE

This policy covers all of our company's information, systems, networks, and other information assets to ensure adequate controls are in place to ensure the confidentiality, integrity and availability of our data. These critical assets must be managed and controlled to protect our company from loss due to misuse, disclosure, fraud, or destruction. This policy applies to all company employees, temporary employees, contractors, consultants, vendors, service providers, partners, affiliates, third parties or any other person or entity authorized to utilize our information resources.

This includes all information systems, hardware, software, data, media, and paper files at our company and any approved third-party facilities. This policy also pertains to all systems, networks, and users connected to our company resources through any means, including but not limited to: local access, leased lines, wireless access points, or any other telecommunications device, through either private or public networks. It also applies to all third-party local and remote connections as well as non-company assets involved in the storage, processing, or transmission of company's information or data.

10.3 POLICY

It is the responsibility of our company's employees, contractors, vendors and agents with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection. General access to the Internet for recreational use through our company network is strictly limited to our employees, guests, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing

our network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users. Performance of illegal activities through our company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see our Access Policy on acceptable use. Authorized Users will not use our networks to access the Internet for outside business interests or any such activities that will harm the business. All remote access connection options, including how to obtain a remote access login/VPN, anti-virus software, troubleshooting will be managed through the BIS technical lead.

10.4 CONNECTION PROCEDURES

1. Secure remote access will be strictly controlled with encryption through our Active Directory Authentication and Virtual Private Networks (VPNs)) with strong passphrases. For further information see our company's Access Policy and Password Policy.
2. Authorized Users shall protect their login and password, even from family members.
3. While using our corporate owned computer to remotely connect to our corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct our company business must be approved in advance by the appropriate HOD.
5. All hosts that are connected to our company's internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement with the partner.
6. Personal equipment used to connect to our company's networks must meet the requirements of company owned equipment for remote access - and approved by the appropriate HOD.

10.5 COMPLIANCE

The Business Information System team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection. The results of this monitoring will be provided to the appropriate HOD. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10.6 EXCEPTION TO POLICY

Any exception to the policy must be approved by the business unit manager

10.7 APPLICABILITY

This policy applies to all company employees, contractors, vendors, and agents with a company owned or personally owned computer or workstation used to connect to our network. This policy applies to remote access connections used to do work on behalf of company, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to our company's networks.

POLICY: DISPOSAL OF BIS EQUIPMENT POLICY	POLICY No: 11
RESPONSIBILITY: ALL INTERESTED PARTIES	EFFECTIVE DATE: 02 October 2023

1. PURPOSE

The purpose of this BIS Disposal Policy is to establish guidelines and procedures for the proper disposal of information technology assets to ensure data security, environmental compliance, and legal adherence.

2. SCOPE

This policy applies to all employees, contractors, and third-party service providers who are involved in the disposal of Business information systems assets owned or used by the organization.

3. POLICY

- No RTG owned BIS equipment (including portable devices) may be disposed of outside the processes set out in this policy. Users with equipment that needs to be disposed of should ensure the safe disposal of that equipment.
- All BIS equipment must be disposed of in accordance with this policy.
- If BIS equipment is disposed of by third party contractors on our behalf, they must adhere to the relevant standards. They must also provide the relevant certificates of destruction and copies of waste consignment notes.
- Where it's physically possible or appropriate, try to witness the secure destruction of the equipment being disposed of.

4. RESPONSIBILITIES

4.1 BIS Department

- Oversee the proper disposal of BIS assets in accordance with this policy.
- BIS will decide whether the equipment can be reallocated or disposed of as appropriate.
- Implement and manage secure data erasure or destruction methods. Before the disposal of computer equipment, all personal and sensitive data must be securely destroyed. This must be using a method appropriate to the risk associated with the sensitivity of data, and the equipment it's stored on.
- Keep an updated inventory of all BIS assets earmarked for disposal.
- BIS to remove all other data and any software licensed to RTG before the equipment leaves the organization's possession.

4.2 Asset Owners:

- Notify the BIS department of any assets that need to be disposed of.

- Ensure that all sensitive information is removed or securely wiped from the devices before disposal in line with this policy.

5 DISPOSAL FORMAT

5.1 Data Sanitization:

- Before disposal, all electronic storage media must undergo a secure data erasure process using approved software.
- Physical destruction of storage media is an acceptable alternative when secure erasure is not possible.

5.2 Asset service life/ useful life:

- Asset to be disposed of after being in use for the below tabulated service life.

ASSET TYPE	YEARS
Laptop	3
Desktop & Monitor	3
Micros Workstations	3
Server	3
Router	3
Switch	3
Printer	3
Projector	3
UPS	3
iPad	2

6 DOCUMENTATION

6.1 Disposal Records:

- Maintain detailed records of all BIS assets earmarked for disposal, including make, model, serial number, and date of disposal.
- Document the method of data sanitization or destruction for each asset.

7 EMPLOYEE TRAINING

All employees involved in the disposal process must undergo training on this policy and the procedures outlined herein.

8 COMPLIANCE WITH REGULATIONS

Ensure compliance with all relevant data protection laws, environmental regulations, and other legal requirements related to IT asset disposal.

9 REVIEW AND UPDATES

This policy will be reviewed annually to ensure its effectiveness and relevance. Updates will be made as necessary to address changes in technology, regulations, or organizational requirements.

10 ENFORCEMENT

Failure to comply with this BIS Disposal Policy may result in disciplinary action.

11 CONTACT INFORMATION

For questions or concerns regarding BIS disposal, contact the BIS department.

12 EXCEPTIONS

Exceptions to the guiding principles in this policy must be documented and formally approved by the BIS Head of Department and Rainbow Tourism Group.

Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required.
- any risks created by the policy exception.
- evidence of approval by all appropriate parties

Title: Change Request Form

1. Change Proposer – General Information				
Proposer Name				
Unit				
Department				
Type of change requested – *Please tick*	System Enhancement		System Bug	
Brief description of request				
Reason for change				
Other department affected by proposed change				
Date Submitted				
Date Required				
Proposer Signature				
Please attach any material/reference that might support your proposal				
2. Business Information Systems Head – Initial Analysis				
Business Case				
BOP Impact				

Vendor/Contractual/Licensing Impact	
Cost Impact	
Comments	
Recommendations	
Signature	
Date	

3. Management Committee - Decision								
Decision	Approve		Approve with conditions		Reject		Need more Information	
Conditions								
Comments								
Chairman Signature								
Date								

Title: Risk Assessment Form

Change Name: _____

Prepared by: _____

Date: _____

Instructions for using this document

Section I Risk Assessment Form

Use Section I of this template to identify risks that will impact the Change and the level of threat they pose to the Change's success. In this section, characteristics are grouped in typical categories of Change risk. High, medium and low risk ratings are assigned to descriptions of each Change characteristic. The list of Change characteristics is not exhaustive and is intended to provide a starting point only. Customize the Form by adding to the list specific risk characteristics or criteria that apply to your organization or Change. To complete the Form, for each characteristic, choose the phrase that best depicts your Change at the time of assessment.

The completed Form will identify the Change's risk factors. The results from the completed Form should be used as guidelines; there may be other factors that will lower or raise the risk level. For instance, a large Change carries with it an inherently higher risk. This risk may be reduced if an experienced Change manager leads the Change. Having many high-risk characteristics does not necessarily mean the Change will fail. However, it does mean that a plan must be into place to address each potential high-risk factor.

Section II Typical High-risk Problems/Response Actions:

Use Section II of this template to analyze identified risks and plan appropriate responses. Early warning signs and examples of problems that may result from certain types of high risks are listed alongside examples of activities that may be undertaken to mitigate or respond to each risk. For each high-risk factor identified in Section I, create a response plan to ensure that the risk is mitigated and does not impact Change success. Consider the example activities in Section II as potential responses. The Change team may suggest additional response actions. After creating response plans for all the high-risk factors, look at the medium-level risks to determine if the impact is severe enough to warrant a risk response plan created for them as well. If so, create a response plan for the medium-risk factors. Low-risk factors may be considered assumptions, that is, there is a potential for problems, but because the risk is low, you are "assuming" that the condition will not occur. The activities associated with responding to the high and medium risk factors should then be captured in the risk response plan. The risk response plan is used throughout the Change to monitor and control risks.

response plans for all the high-risk factors, look at the medium-level risks to determine if the impact is severe enough to warrant a risk response plan created for them as well. If so, create a response plan for the medium-risk factors. Low-risk factors may be considered assumptions, that is, there is a potential for problems, but because the risk is low, you are "assuming" that the condition will not occur. The activities associated with responding to the high and medium risk factors should then be captured in the risk response plan. The risk response plan is used throughout the Change to monitor and control risks.

Section I - Risk Assessment Form:				
	Characteristics	Low risk	Medium risk	High risk
A. Scope				
A1	The scope of the Change is:	Well defined & understood	Somewhat defined, but subject to change	Poorly defined and/or likely to change
A2.	The business requirements of the Change are:	Understood and straightforward		Very vague or very complex
A3.	The system availability requirements include:	Windows of availability and downtime		Availability on a 24/7 basis
A4.	The total estimated effort hours are:	Less than 1,000		Greater than 5,000
A5.	The quality of current data is:	Well defined and simple to convert		Poor or complex to convert
A6.	If a package implementation:	No (or minimal) customization is needed		Heavy customization is needed
A7.	If a package implementation:	The product or release is stable		The product or release is new to the market

Section I - Risk Assessment Form:				
	Characteristics	**Low risk**	**Medium risk**	**High risk**
B. Schedule				
Are the Change's major milestones and operational dates:		Flexible - may be established by the Change team and recipient personnel	Firm - pre-established and missed dates may affect the business	Fixed - pre-established by a specific operational commitment or legal requirements beyond the team's control
B2.	Change duration is estimated at:	Less than 3 months	3 months to 12 months	Greater than 12 months
C. Budget				
The Change budget is based upon use of a proven successful cost estimation process used by personnel with estimation experience:		Yes – Proven estimation process with experienced personnel	Some experience or process	No – Estimates not established by personnel with any experience nor any proven process
Change funding matches or exceeds the estimated		Funding is greater than	Funding is marginally	Funding is less than

A6.	If a package implementation:	No (or minimal) customization is needed		Heavy customization is needed
A7.	If a package implementation:	The product or release is stable		The product or release is new to the market

Section I - Risk Assessment Form:				
	Characteristics	**Low risk**	**Medium risk**	**High risk**
B. Schedule				
	Are the Change's major milestones and operational dates:	Flexible - may be established by the Change team and recipient personnel	Firm - pre-established and missed dates may affect the business	Fixed - pre-established by a specific operational commitment or legal requirements beyond the team's control
B2.	Change duration is estimated at:	Less than 3 months	3 months to 12 months	Greater than 12 months
C. Budget				
	The Change budget is based upon use of a proven successful cost estimation process used by personnel with estimation experience:	Yes – Proven estimation process with experienced personnel	Some experience or process	No – Estimates not established by personnel with any experience nor any proven process
	Change funding matches or exceeds the estimated cost and is stable.	Funding is greater than estimated need and/or is expected to be stable.	Funding is marginally adequate and expected to remain relatively stable.	Funding is less than estimated need and/or its stability is highly uncertain.
D. Change Linkages				
	This Change's dependencies on linkage Changes could best be described as:	Slightly dependent, can be successful without linkage Change deliverables	Somewhat dependent, without linkage Change deliverables, schedule delays possible	Highly dependent, cannot proceed without deliverables from linkage Changes
E. Human Resources				
E1.	The Change Manager's experience and training is:	Recent success in managing changes similar to this one	Recent success in managing a Change not similar to this one or trained and no actual experience	No recent experience or Change management training

Section I - Risk Assessment Form:				
	Characteristics	**Low risk**	**Medium risk**	**High risk**
E2.	Describe the experience of Change personnel with the tools and techniques to be used.	Experienced in use of tools and techniques	Formal training in use of tools and techniques but little or no practical experience	No formal training or practical experience in use of tools and techniques
E3.	The Change team is:	Located together		Dispersed at multiple sites
F. Management/Senior Leadership Support				
	F1. The Change sponsor is:	Identified, committed, and enthusiastic		Not identified or not enthusiastic

Change funding matches or exceeds the estimated cost and is stable.	Funding is greater than estimated need and/or is expected to be stable.	Funding is marginally adequate and expected to remain relatively stable.	Funding is less than estimated need and/or its stability is highly uncertain.
D. Change Linkages This Change's dependencies on linkage Changes could best be described as:	Slightly dependent, can be successful without linkage Change deliverables	Somewhat dependent, without linkage Change deliverables, schedule delays possible	Highly dependent, cannot proceed without deliverables from linkage Changes
E. Human Resources E1. The Change Manager's experience and training is:	Recent success in managing changes similar to this one	Recent success in managing a Change not similar to this one or trained and no actual experience	No recent experience or Change management training

Section I - Risk Assessment Form:			
Characteristics	**Low risk**	**Medium risk**	**High risk**
E2. Describe the experience of Change personnel with the tools and techniques to be used.	Experienced in use of tools and techniques	Formal training in use of tools and techniques but little or no practical experience	No formal training or practical experience in use of tools and techniques
E3. The Change team is:	Located together		Dispersed at multiple sites
F. Management/Senior Leadership Support F1. The Change sponsor is:	Identified, committed, and enthusiastic		Not identified or not enthusiastic
G. Business or Organizational Impacts			
G1. The Change participant(s) providing content knowledge on the Change:	Are not required on the Change or are very knowledgeable	Are somewhat inexperienced	May not be available as needed or are unknown at this time
G2 Business processes, procedures, policies require:	Little or no change	Occasional to frequent changes	Substantial change
G3. Describe the impact on business procedure, process, or organizational changes as a result of this Change:	Either none or only minor changes of procedural, process, or organization	Moderate procedural, process, or organizational changes	Major procedural, process, or organizational changes or unknown at this time
G4. The number of organizations this will affect is:	One or two	Three or four	More than five
G5. How would you rate the readiness level within the Change recipient and stakeholder organizations for changes this Change will create?	High readiness (Passionate and enthusiastic)	Moderate readiness	Low readiness (Passive and hard to engage)

Section I - Risk Assessment Form:			
Characteristics	**Low risk**	**Medium risk**	**High risk**
H. Technology			
H1. The technology being utilized consists of:	Mature (Existing software, hardware, languages, databases, and tools)	Emerging	Leading Edge (New software, hardware, languages, databases, or tools (or new releases))
H2. The technical requirements are:	Similar to others in the company		New and complex

G5.	How would you rate the readiness level within the Change recipient and stakeholder organizations for changes this Change will create?	High readiness (Passionate and enthusiastic)	Moderate readiness	Low readiness (Passive and hard to engage)

Section I - Risk Assessment Form:				
	Characteristics	**Low risk**	**Medium risk**	**High risk**
H. Technology				
H1.	The technology being utilized consists of:	Mature (Existing software, hardware, languages, databases, and tools)	Emerging	Leading Edge (New software, hardware, languages, databases, or tools (or new releases))
H2.	The technical requirements are:	Similar to others in the company		New and complex
H3.	The subject matter is:	Well known by the Change team		Not well known by the Change team
I.	**Vendor**			
I1.	If a package implementation:	The vendor is familiar in this market	Yes – Some contractors are required (less than 50%) and are expected to be signed before start of Change	The vendor is new to this market
I2.	Are contractors required and committed to the Change?	No – Contractors are not required		Yes – Change will be staffed by over 50 % contractors and/or contractors' commitment is not expected to be complete prior to start of change
J. Other (Add as appropriate to Change)				
J1.				

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A1.	**The scope of the Change is poorly defined** • Hard to provide sound estimates • May spend time and cost on areas out of scope • Hard to gather concise requirement • Difficult to write Change definition and work plan • Hard to invoke scope-change procedures • Change deliverables are poorly defined	• Focus on firming up scope in the planning process • Define various components of scope, such as what organizations are affected, what deliverables are expected, what type of information is required • Clearly define what is out of scope for the Change • Begin to define business requirements at a high level and then work upward to define scope • Ask Change sponsor to make decision on conflicting scope statements • Document all scope assumptions when providing estimates of work, cost, or duration • Use pictures or diagrams to communicate scope and options • Establish firm scope-change procedures up front • Ensure the Change definition and business requirements are formally approved and signed off on • Distribute scope statements to all stakeholders for confirmation • Do not begin Change until scope is clear
A2.	**The business requirements of the Change are vague or complex** • Difficult to document the requirement properly	• Use joint application design (JAD) session to gather requirements from all stakeholders together • Utilize prototyping and iterative development techniques to assist users in

Section I - Risk Assessment Form:

	Characteristics	Low risk	Medium risk	High risk
H.	**Technology**			
H1.	The technology being utilized consists of:	Mature (Existing software, hardware, languages, databases, and tools)	Emerging	Leading Edge (New software, hardware, languages, databases, or tools (or new releases))
H2.	The technical requirements are:	Similar to others in the company		New and complex
H3.	The subject matter is:	Well known by the Change team		Not well known by the Change team
I.	**Vendor**			
I1.	If a package implementation:	The vendor is familiar in this market	Yes – Some contractors are required (less than 50%) and are expected to be signed before start of Change	The vendor is new to this market
I2.	Are contractors required and committed to the Change?	No – Contractors are not required		Yes – Change will be staffed by over 50 % contractors and/or contractors' commitment is not expected to be complete prior to start of change
J.	**Other (Add as appropriate to Change)**			
J1.				

Section II—Typical high-risk Problems/Response Actions:

	High-risk factors/ Potential problems	Risk Response Actions
A1.	**The scope of the Change is poorly defined** • Hard to provide sound estimates • May spend time and cost on areas out of scope • Hard to gather concise requirement • Difficult to write Change definition and work plan • Hard to invoke scope-change procedures • Change deliverables are poorly defined	• Focus on firming up scope in the planning process • Define various components of scope, such as what organizations are affected, what deliverables are expected, what type of information is required • Clearly define what is out of scope for the Change • Begin to define business requirements at a high level and then work upward to define scope • Ask Change sponsor to make decision on conflicting scope statements • Document all scope assumptions when providing estimates of work, cost, or duration • Use pictures or diagrams to communicate scope and options • Establish firm scope-change procedures up front • Ensure the Change definition and business requirements are formally approved and signed off on • Distribute scope statements to all stakeholders for confirmation • Do not begin Change until scope is clear
A2.	**The business requirements of the Change are vague or complex** • Difficult to document the requirement properly • Difficult to use tools to document the requirements • Difficult to understand what the expectations of the Change are • Chance that the resulting solution will not meet business need • May be a sign of a lack of focus from the customer	• Use joint application design (JAD) session to gather requirements from all stakeholders together • Utilize prototyping and iterative development techniques to assist users in discovering the requirements of the new system • Get access to the sponsor and to senior management to provide overall guidance • Provide training to the customers on how to think about and express business requirements • Ensure that the final business requirements are approved in writing and that a change-management procedure is enforced after that

A2.	**The business requirements of the Change are vague or complex** • Difficult to document the requirement properly • Difficult to use tools to document the requirements • Difficult to understand what the expectations of the Change are • Chance that the resulting solution will not meet business need • May be a sign of a lack of focus from the customer	• Use joint application design (JAD) session to gather requirements from all stakeholders together • Utilize prototyping and iterative development techniques to assist users in discovering the requirements of the new system • Get access to the sponsor and to senior management to provide overall guidance • Provide training to the customers on how to think about and express business requirements • Ensure that the final business requirements are approved in writing and that a change-management procedure is enforced after that

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A3.	**The system availability requirements are 24/7** • Downtime problems may result in productivity decreases or loss of revenue • Redundancy may be needed, which increases system complexities • Newer advanced technology may be required • More procedures and processes are needed to maintain the system environment	• Allocate more time to analysis, design, testing, and overall quality assurance activities • Focus extra time and energy on technology architecture • Focus more time and energy on database design • Use industry best practices for all technology and process components • Provide appropriate training to the team so they understand the 24/7 implications on the Change • Determine exactly what portions of the system have a 24/7 requirement • Look for internal or outside experts to validate overall technical design and architecture • Develop solid disaster recovery procedures • Develop a strong partnership with the hardware and software vendors

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A4.	**High number of estimated effort hours** • Implication of a high number of effort hours is that there are many people involved and more complexity • Harder to communicate effectively with the team • Bottlenecks can occur when decisions are needed quickly • More chance of people problems • Increased chance of turnover • More people to train	• Use a Change management tool to control resource utilization • Have team members utilize weekly status reports to report on progress against their assigned work plan activities • Utilize team leaders to manage sub teams • Organize team-building activities to build cohesion • Schedule status meetings to keep people informed of Change status

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A4.	**High number of estimated effort hours** • Implication of a high number of effort hours is that there are many people involved and more complexity • Harder to communicate effectively with the team • Bottlenecks can occur when decisions are needed quickly • More chance of people problems • Increased chance of turnover • More people to train	• Use a Change management tool to control resource utilization • Have team members utilize weekly status reports to report on progress against their assigned work plan activities • Utilize team leaders to manage sub teams • Organize team-building activities to build cohesion • Schedule status meetings to keep people informed of Change status • Utilize structured internal procedures for scope, issue, quality, and risk management • Break the Change into smaller, shorter sub changes • Reduce available Change work time per person, per day to recognize additional people and team-related activities
A5.	**The quality of current data is poor and difficult to convert** • More work to convert the old data to the new system • Scrubbed data may still cause problems in the new system • Data conversion problems can cause significant Change delays	• Make sure that all the old data elements are correctly mapped to the new system • Test the conversion process out rigorously before proceeding with final conversion • Determine if the cost and trouble associated with the converted data is worth the value. Ask whether the new system can start with new data only. • Keep the old system around for some period to access the old data • Spend the effort to manually clean up the old data as much as possible before conversion

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A6.	**Package implementation requires heavy customization** • Customization brings added complexity to the Change • Making modifications may result in something else breaking • Customization can lead to poor performance • Customization can complicate migrating to newer releases • Heavy customization may mean that the wrong package was selected • Package will probably take longer to implement • Customization will require more reliance on the vendor	• Consider other packages • Consider custom development • Cut back on the business requirements so that customizations are not required • Get a firm estimate of the cost and duration of the modifications from the vendor and build into your overall work plan • Manage the vendor relationship to ensure all needed work is completed on schedule • Make sure the sponsor has approved the customizations

	• More people to train	• Schedule status meetings to keep people informed of Change status • Utilize structured internal procedures for scope, issue, quality, and risk management • Break the Change into smaller, shorter sub changes • Reduce available Change work time per person, per day to recognize additional people and team-related activities
A5.	**The quality of current data is poor and difficult to convert** • More work to convert the old data to the new system • Scrubbed data may still cause problems in the new system • Data conversion problems can cause significant Change delays	• Make sure that all the old data elements are correctly mapped to the new system • Test the conversion process out rigorously before proceeding with final conversion • Determine if the cost and trouble associated with the converted data is worth the value. Ask whether the new system can start with new data only. • Keep the old system around for some period to access the old data • Spend the effort to manually clean up the old data as much as possible before conversion

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
A6.	**Package implementation requires heavy customization** • Customization brings added complexity to the Change • Making modifications may result in something else breaking • Customization can lead to poor performance • Customization can complicate migrating to newer releases • Heavy customization may mean that the wrong package was selected • Package will probably take longer to implement • Customization will require more reliance on the vendor	• Consider other packages • Consider custom development • Cut back on the business requirements so that customizations are not required • Get a firm estimate of the cost and duration of the modifications from the vendor and build into your overall work plan • Manage the vendor relationship to ensure all needed work is completed on schedule • Make sure the sponsor has approved the customizations being proposed • Thoroughly test the modified package for functionality and performance • Maintain a vendor log to track issues and milestones
A7.	**Package implementation is a new product or release** • Greater chance of problems surfacing • More reliance on the vendor to ensure problems are corrected quickly • Installation, testing, and deployment will take longer • Hard to know up front whether the package meets all the business requirements	• Schedule training on the package as early in the Change as possible • Add an internal resource, or a consultant, with prior product experience onto the Change • Schedule a pilot test or a prototype to gain familiarity with the package before full implementation • Establish agreements with the vendor stipulating support level and problem resolution times • See if the Change can be delayed until other companies have utilized the product • Seek out other companies that have used the product for their feedback and key learnings

B. Schedule		
Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
B1.	**The Changes major milestones and/or operational dates are fixed. They were pre-established by an operational commitment or legal requirements beyond control of the Change team**	• Re-negotiate schedule requirement to fit required activities. • Re-negotiate scope to limit to activities deemed doable

B. Schedule		
Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
B1.	**The Changes major milestones and/or operational dates are fixed. They were pre-established by an operational commitment or legal requirements beyond control of the Change team.** • Work must be scheduled to fit within this schedule constraint • Given schedule window may be impossible to accommodate required activities • Most likely the schedule requirements will be impossible to meet • Hurried activity and schedule pressures are likely to cause inadvertent errors in work	• Re-negotiate schedule requirement to fit required activities. • Re-negotiate scope to limit to activities deemed doable in allotted time. • Establish new agreements with Customer/Owner/Sponsor based upon realistic estimates • Put aggressive Change tracking and monitoring plans in place • Communicate status reports on regular basis
B2.	**Long estimated Change duration** • Harder to manage the schedule • Easier for the team and the customer to drift or lose focus • More chance that Change will lose organizational commitment • More chance business requirements will change • More chance of change in software or hardware versions • Difficult to instil sense of urgency at the beginning of Change • More chance of team and customer turnover	• Break the Change into smaller, shorter sub changes • Identify clear milestones to check that the Change is on schedule • Be diligent using formal change management procedures • Rotate team members into different roles to keep up the interest level • Strive to get ahead of schedule as early as possible. • Instil a sense of urgency from the start of the Change • Organize team-building activities to build cohesion and reduce friction • Ensure all major deliverables are formally approved, so that change management can be invoked afterward • Make technical design and architecture decisions as flexible as possible to account for potential changes

C. Budget		
Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
C1.	**Change budget was not established with any proven tool or by any experienced person.** • Budget will most likely not be accurate • Budget will not be structured in manor to facilitate tracking and control. • There will be unrealistic expectations for what can be accomplished within the budget.	• Re-estimate the Change using proven tools and experienced personnel • Revise scope to fit within the funding available • Don't start the Change until a better budget can be established
C2.	**Change funding is less than the estimated cost and is unstable.** • Change will be unable to fulfil expectations • Change will likely exceed it's funding	• Renegotiate scope to fit within the funding available • Don't start the Change until an adequate budget or lesser scope is established
D. Change Linkages		
D1.	**The Change is highly dependent upon and cannot proceed without first • for receiving completed deliverables form another separate linkage** • Things out the control of this Change can adversely affect this schedule and ability to be successful • Establish agreement with the linkage site to • Delays in linkage Change deliverables are likely to cause similar increased Change probability or delays in this Change's schedule • Close monitoring and coordination of both Changes needs to be performed to minimize impact of the conflict.	Pursue revising either or both Change schedules to allow **Change** alignment of Change deliverables. Change's outcome • Re-negotiate scope and/or fulfil this Change's delays and needs and document the agreement

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
E	**Human Resource**	
E1.	**Change management experience is light** • May take longer to define the Change and build work plan • May make more mistakes in judgment, causing rework and Change delays • More difficulty organizing and managing a complex Change • May not be familiar with sound Change management practices • May not know when to call for help	• Provide up-front Change management training • Designate a more senior person to coach and mentor the Change manager • Break the Change into smaller pieces that are easier to manage • Put a strong quality-assurance process in place to ensure the Change is on the right track • Make sure the major deliverables are formally approved • Utilize strong team leaders and team members to bring additional experience to bear
E2.	**Change management processes are unfamiliar or will not be used** • Team may have a difficult time understanding how to raise issues, scope changes, and risks • Change may get out of control as the internal processes become more complex and harder to manage • Communication will tend to be poorer • Change deliverables might be completed in different formats • Issues may not be addressed in a timely manner, scope changes may be adopted without thought of impact to the Change, risks may be ignored, and quality may be compromised • Chance that the Change may be in trouble before it is recognized	• Provide training to the Change manager and Change team on sound Change management processes and procedures • Assign an experienced Change management coach or mentor to the Change • Break the Change into smaller pieces that can be managed with less-rigorous Change management • Define and gain approval for a set of Change management procedures before the Change starts, including issues management, change management, risk management, and quality management • Create a solid communication plan to ensure everyone knows what's going on and can provide feedback • Solicit input on issues, risk, scope change, and quality concerns on an ongoing basis

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
E3.	**Change team is located in dispersed locations** • Harder to communicate effectively • Less team interaction and cohesion • Harder to build personal relationship with the entire team • Some members may feel isolated and not a part of the team • Technology problems may result in productivity decrease	• Try to get the team into one location, at least for the length of the Change • Create an aggressive communication plan to ensure the team communicates effectively • Hold regular meetings where the entire team meets face-to face • Schedule team-building activities where the entire team meets face-to-face • Have backup methods to communicate if the primary technology fails • Maintain frequent contact by phone with remote team members • Create a central repository to hold the Change documentation that all team members can access
F.	**Management/Senior Leadership Support**	
	F1. The Change sponsor is not identified or not enthusiastic • Change may not get the resources it needs • Change may not have the long-term commitment needed • Issues and change requests may not be resolved in a timely manner • Don't start the Change	• Establish a strong steering committee to help guide the Change • Establish a process for resolving disputes between political battles may delay the Change organizations • Try to identify a different sponsor • Ask the sponsor to delegate full authority to another person who can act on their behalf
G.	**Business or Organizational Impacts**	
G1.	**The Change participant(s) providing content knowledge are either not available or not identified at this time.** • Lack of content knowledge available to the Change will adversely affect the ability to accurately complete the Change • Change recipients will not be pleased with the Change	Re-negotiate resource commitments to make content knowledge available to the Change. Re-negotiate schedule to obtain required content knowledge Don't start the Change

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
G2.	**Business processes and policies require substantial change** • Policy changes could delay the Change • People will be confused with new processes, which will affect their ability to utilize the solution • Possibility that new processes will not be fully integrated at first • Possible void if new processes don't fully cover all contingencies • System functions may not be used if not supported by correct procedures • Substantial change in processes may result in destructive behaviour	• Document all current policies and processes and ensure that they are correct • Communicate precisely how the new processes differ from the old ones • Communicate potential changes as far in advance as possible • Ensure the customers are defining the process and policy changes • Have one person responsible for all process and policy changes • Create an aggressive communication plan to keep customers engaged and informed • Use the new processes in a pilot test or prototype first to ensure they are workable and correct • Include the successful implementation of new policies and processes as part of the performance criteria for managers • Be open to customer input on process changes—for better ideas and to allow them to feel they have impact
G3.	**Changes to organization structure are substantial** • Organizational uncertainty can cause fear in the organization • People may not focus on Change if they have organizational concerns • People may fear loss of jobs in a new organization • People may not use the system if they are unhappy with the organizational change • Uncertainty may cause decisions to be delayed • Organizational change may result in decisions made for political purposes	• Document the concerns that come out of a new organization and look for ways to mitigate the concerns • Communicate early and often about the potential for change and the business reasons for it • Involve representatives from all stakeholder areas in the organizational design and options • Get human resources involved to deal with potential people issues

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
G4.	**High number of organizations are affected** • Coordination is more complex • Approvals can be more cumbersome and lengthy • More difficult to reach consensus • More people and groups to involve in planning and requirements • Harder to know the major stakeholders of the various organizations • Implementation is harder and more complex	• Establish a formal approval process • Create a steering committee to represent the entire stakeholder community • Keep the sponsor engaged and ready to intervene in the various organizations • Include representative from each organization in requirements, quality assurance, and testing • Include opportunities for people from the various organizations to meet and interact • Work with the team on strict adherence to overall Change objectives and priorities • Use consensus-building techniques when at all possible
G5.	**Customer commitment level is passive/hard to engage** • May point out low confidence in the business value • Harder to get customer time and resources needed • Harder to gather business requirements • Customers may undermine or work against the Change	• Create an aggressive communication plan to keep customers engaged and communicate the business benefit • Create user group to surface concerns and build enthusiasm • Ask for customer participation in planning and requirements gathering • Ask for help from the sponsor to generate excitement • Look for opportunities to sell Change in fun settings and contexts • Be proactive in gaining commitments for customer resources when you need them • Don't start the Change

H. Technology		
Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
H1.	**The Change technology is new and unfamiliar (or new releases)** • Learning curve may result in lower initial productivity • May be integration problems between old and new technology • Resistance to technology changes may cause the Change to be delayed • May be difficulty testing the new technology • Technology may not be installed or configured correctly, which will lead to Change delays • New tools can lead to longer delivery times • New technology may require substantial conversion efforts • System performance may be poor while expertise is gained in optimizing and configuring the technology	• Provide as much training on the new technology as practical, as early as possible • Train everyone who needs to install, use, or support the new technology • Make arrangements to rely on vendor technical specialists, when needed • Use outside consultants who are familiar with the technology • Make sure there is an adequate test environment where the technology can be utilized without affecting production • Ensure that solid analysis is completed regarding the new technology functions, features, and capabilities • Create procedures and standards for how the new technology should be utilized • Create a pilot test or prototype to utilize the new technology in a small way at first

Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
H2.	**The technical requirements are new and complex** • May be difficult to understand the requirements and the implications of design decisions • May be integration issues between old and new technology • May be difficulty testing the complex technology • The more complex the technology, the greater the risk that problems will occur • Problems with incompatible technologies may not be uncovered until integration or system testing	• Utilize system and technical design documents to clearly lay out how the technology fits together • Define the overall system technical architecture and have it approved by knowledgeable people in your company • Send the architecture proposal to outside consultants for further feedback and validation • Create a pilot test or prototype to utilize the new technology in a small way at first • Try to substitute more proven and familiar technology in the architecture • Utilize multiple products from the same vendor to ease integration complexities • Use products that utilize open standards and architectures to reduce the risk of integration problems
H3.	**Subject matter is not well known by the Change team** • Longer learning curve for Change team members • The Change may slip behind in the early portions of the Change • No sense for whether business requirements make sense • Possibility that critical features or functions will be missed • Need to initially rely on customer for all subject-matter expertise	• Take as much training as practical, as early on as possible • Bring the key customers onto the Change team • Spend extra time understanding and documenting the requirements • Set up approval process for requirements that require multiple subject-matter experts • Use joint application design (JAD) session to gather requirements from all stakeholders together • Utilize more frequent walkthroughs and include the users • Build extra time into the estimates for application analysis and design activities.

H2.	**The technical requirements are new and complex** • May be difficult to understand the requirements and the implications of design decisions • May be integration issues between old and new technology • May be difficulty testing the complex technology • The more complex the technology, the greater the risk that problems will occur • Problems with incompatible technologies may not be uncovered until integration or system testing	• Utilize system and technical design documents to clearly lay out how the technology fits together • Define the overall system technical architecture and have it approved by knowledgeable people in your company • Send the architecture proposal to outside consultants for further feedback and validation • Create a pilot test or prototype to utilize the new technology in a small way at first • Try to substitute more proven and familiar technology in the architecture • Utilize multiple products from the same vendor to ease integration complexities • Use products that utilize open standards and architectures to reduce the risk of integration problems
H3.	**Subject matter is not well known by the Change team** • Longer learning curve for Change team members • The Change may slip behind in the early portions of the Change • No sense for whether business requirements make sense • Possibility that critical features or functions will be missed • Need to initially rely on customer for all subject-matter expertise	• Take as much training as practical, as early on as possible • Bring the key customers onto the Change team • Spend extra time understanding and documenting the requirements • Set up approval process for requirements that require multiple subject-matter experts • Use joint application design (JAD) session to gather requirements from all stakeholders together • Utilize more frequent walkthroughs and include the users • Build extra time into the estimates for application analysis and design activities.

I. Vendor		
Section II—Typical high-risk Problems/Response Actions:		
	High-risk factors/ Potential problems	**Risk Response Actions**
I1.	**Package implementation is from a new vendor** • Possibility that vendor may not survive and leave you with no support • Upgrades may be in jeopardy if there are not enough sales in the marketplace • No prior relationships from which to build a quick partnership • Legal and financial concerns may delay contracts and the Change	• Make sure that all agreements with the vendor be in writing • Insist that source code be placed in escrow in case the company does not survive • Ask the vendor to be a part of the Change team • Maintain a vendor log to track problems with the package • Make sure the vendor is financially sound • Establish agreements with the vendor stipulating support level and problem resolution times
I2.	**Change requires over 50% contractors who may not yet be committed to the Change?** • Change lacking required staff at start • Schedule will be adversely impacted	• Increase Change management oversight of contractor personnel • Start of Change should be delayed until staffed • Increased communications focus is a must
J. Other (add as appropriate to Change)		
J1.		

POLICY: ONLINE MEETINGS POLICY	POLICY No: 11
RESPONSIBILITY: ALL RTG ASSOCIATES	EFFECTIVE DATE: 02 October 2023

11.0 PURPOSE

This document is intended to provide details on the handling of online meetings professionally by associates of RTG Limited and its subsidiaries Gateway Stream, Gateway Stream Music and Heritage Expeditions Africa.

11.1 SCOPE

The intended recipients of this policy are Associates of RTG Limited and all its subsidiaries. The host is responsible for initiating online meetings (Zoom/Microsoft Teams). RTG Ltd online meetings will only have one host per meeting although there can be multiple co-hosts.

11.2 POLICY

In enforcing Covid-19 guidelines of minimizing the spread of the virus, RTG Ltd recognizes that the holding of online meetings (Zoom/Microsoft Teams meetings) is a critical communication channel to the operations of the respective departments in upholding social distance. It is essential that certain basic standard practices be followed to ensure that professionalism is upheld during the holding of zoom meetings.

11.3 PROCEDURE

11.3.1 Preparation before a meeting

- Host to ensure that goal of meeting is clear.
- Advise participants of your intention to hold a zoom meeting at least 24 hours before the meeting and advise them of the following:
  - Agenda (preparatory notes for participants)
  - Zoom link including time to check in.
  - Duration of meeting
  - Participants to the meeting
  - All required attachments and presentations must be clear and within ease of reach, preferably in a folder named after the meeting.
- Host/ participant to ensure environment is conducive for a meeting to be held. Environment must be:
  - Free from noise
  - Free from disruptive decorum.
  - Neat and exude professionalism.
- Host/ participant to desist from undertaking disturbing behaviours such as eating, cooking, dressing amongst others whilst video is on.
- Host/participant to ensure that their dressing is appropriate for meeting.
- All parties must be prepared, focused, and ready to be engaged whether one is the host/participant.

- Host must open meeting access 10 minutes before the meeting start time.
- Attendants must log on 5 minutes before the start time of the meeting.

11.3.2 During the Meeting

- Upon clicking the link, participant will be placed in waiting room and will only enter session once host/co-host lets you in.
- Host to activate video on. Participants are also encouraged to have their video links on, however option to deactivate video can be selected where there are connectivity challenges.
- Host must acknowledge all participants as they become visible for the group meeting.
- Host may start meeting with small chat/or can appoint a member of the participants to "break the ice".
- Host/Chairperson must avail comfort breaks throughout the meeting preferably after 1 hour of discussions for a minimum of 11 minutes.
- Host/Chairperson must avail 5-minute wellness interludes for participants to get up and stretch.
- Host can mute all participants or can request participants to mute themselves.
- Host can advise participants whether meeting will be recorded or not and advise how they can access the recording. Saved recorded meeting becomes a record/ or evidence of meeting.
- Host to encourage participation from participants and have eyes on zoom dashboard for messages and notifications. Participants with contributions to "raise hand up" so that host can select them. It is impolite to interrupt host or other participants speaking.
- Participants must show a 'thumbs up' either using zoom e-tools (reactions emoji's) or physical hand on the video as acknowledgement of discussion points.
- Host/Participants can use the chat tool to post comments related to the agenda/discussion points or information of relevance to the discourse.
- Stick to the agenda and avoid baseless discussions.
- Host must enable sharing tool for presentations and notes to be shared. Presentations must be clear and participants advised before they are shown.
- Ensure all participants are present and following the discussion at hand by regularly inviting comments and randomly calling individual participants.

11.3.3 After the Meeting

- Recap agenda and discuss action items agreed on.
- Solicit for feedback and comments. Ensure all participants are engaged in the discussions and give their own opinions.
- Advise participants how to access recording of the meeting.
- Allow participants to exit the discussion platform and the host to exit last to ensure that no questions are left unanswered.

11.4 Illustrations

1. 2. 3. 4. 5. 6. 7. 8.

1. Mute/unmute button; ensure button is on mute all the time, only unmute to comment.
2. Video button; All RTG Ltd meetings must be attended with video on unless Chairperson of the meeting advises otherwise.
3. Participants; click to view all participants in the meeting.
4. Chat; Use chat tool where necessary especially when experiencing connectivity problems.
5. Share screen; Use tool to share documents. Remove share once presentation comes to an end.
6. Record; Host may record meeting using this tool.
7. Reactions; Click to access emoji's which include thumbs up, laughing, surprise, wave, clapping, celebrating.
8. Leave; Click to leave the meeting.

POLICY: DATA BACKUP AND RECOVERY POLICY	POLICY No: 12
RESPONSIBILITY: ALL BIS ASSOCIATES	EFFECTIVE DATE: 02 October 2023

12.0 PURPOSE

This document is intended to provide details on the stipulations of data backup and retrieval operations to the RTG Limited.

12.1 SCOPE

The intended recipients of this policy are Associates in the BIS Department at RTG Limited. The Systems Administrator is responsible for the backup and restore procedures run.

12.2 POLICY

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

The GFS (Grandfather-Father-Son) rotation for backups is used.

- Daily Backups (Son) take place on a seven-day rotation.
- Weekly Backups (Father) take place on a four-week rotation.
- Monthly Backups of high availability servers occur the last calendar day of the month and are on a twelve-month rotation.
- Special backups may be made for longer retention periods during special situations such as system upgrades and major projects.

12.3 PROCEDURE

The backup procedure is centered along the Cobian/Veeam backup agent.

12.3.1 Configuring the Backup Agent

The backup plan is configured on the Cobian/Veeam system as follows;

- Select the frequency of backups – daily/weekly/monthly.
- Select files for backups.
- Select the destination folder, this will be the folders residing on the backup server at the disaster recovery site (New Ambassador Hotel)
- Select the encryption method.
- Schedule the backup.

12.3.2 Daily Backups

Use the daily backup schedule form to record the daily backup task.

- Complete the date and time the backup was ran.

- Complete the backup location: (This is the Day's Backup Drive attached to the Backup Server at the Main Data Centre.
- Complete in the status of the backup ran.
- Append signature in the done by column.
- The verifier appends signature in the verification column.
- Move the Day's Backup Drive to the Safe residing at the New Ambassador Hotel DR Site.
- Attach the following Day's Backup Drive to the Backup Server residing at the Main Data Centre in preparation for the day's backup.

12.3.3 Weekly Backups

Use the daily backup schedule form to record the weekly backup task.

- Complete the week no.
- Complete the year
- Complete the backup location – (This should be a folder at the backup server at the disaster recovery site.
- Complete in the status of the backup ran.
- Append signature in the done by column
- The verifier appends signature in the verification column.

12.3.4 Monthly Backups

Use the daily backup schedule form to record the monthly backup task.

- Complete the month
- Complete the year
- Complete the backup location – (This should be a folder at the backup server at the disaster recovery site.
- Complete in the status of the backup ran.
- Append signature in the done by column
- The verifier appends signature in the verification column.

12.3.5 Backup Content

The following system's is covered by the backup policy

- Opera System
- Micros System
- Sage 300
- Belina Payroll
- Microsoft Exchange Mailboxes
- Microsoft SharePoint Data
- RTG Entertainment Card Solution Data
- Materials Control

12.3.6 Backup Types

12.3.6.1 Full backup

Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one **full** backup will be done once a week followed by **differential** and/or **incremental**.

12.3.6.2 Differential backups

Includes files that have been changed since the last Full (Clear Archive Bit) or Incremental backup. If the archive bit is on, the file is backed up, and archive bit is not turned off. The next time an incremental backup is done, this file is skipped (unless it is modified again).

12.3.6.3 Incremental backups

Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).

12.3.7 Backup Media

12.3.7.1 Files

These are Cobian compressed and encrypted files on the backup safe at the Disaster Recovery Site at New Ambassador Hotel

12.3.7.2 External Hard Drives

These are Daily, Weekly and Monthly full backups stored in the safe at the disaster recovery site at New Ambassador Hotel

12.3.8 Recovery Procedures

12.3.8.1 The Recovery Time Objective and Recovery Point Objective

The following table shows the RTOs and RPOs for all the systems in use by RTG Ltd.

System	RTO	RPO
Email	30 minutes	2 hours
Opera	30 minutes	24 hours
Micros	30 minutes	24 hours
VingCard	30 minutes	24 hours
VOIP	30 minutes	2 hours
Midas	30 minutes	24 hours
Sage 300	1 hour	24 hours
Belina Payroll	2 hours	24 hours
Microsoft Office	2 hours	24 hours
SharePoint	2 hours	24 hours

12.3.9 Types of recovery

12.3.9.1 Emergency recovery

Information Technology department will make every attempt to recover the data within the Recovery Time Objective and Recovery Point Objective as specified above.

12.3.9.2 Verification recovery

These restores are done as a control measure to check if the backup set can be used for recovery in the event of a disaster.

The verification restores are performed on a backup set to validate if the backup run has been successful. The system administrator is responsible for the verification restores run.

The verification restores are done three times a week for the daily backup sets and twice a month for the weekly backup sets and quarterly for the monthly backups sets.

12.3.9.3 Requested recovery

Users that need files restored must complete the data recovery request form and submit to the Head- Business Information Systems. The detail of the request should include information about the data file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

The data recovered will be as per the RTO and RPOs specified above.

POLICY #12: DATA BACKUP AND RECOVERY	DEPARTMENT: BUSINESS INFORMATION SYSTEMS	PAGE: 1 of 7

Title: Daily Backup Checklist

Daily Backup Checklist for_____ System

Date	Time	Backup Location	Status	Done By	Verified By

POLICY #12: DATA BACKUP AND RECOVERY	DEPARTMENT: BUSINESS INFORMATION SYSTEMS	PAGE: 2 of 7

Title: Weekly Backup Schedule

Weekly Backup Schedule for_____ System

Week No	Year	Backup Location	Status	Done By	Verified By

Title: Monthly Backup Checklist

Monthly Backup Checklist for_____ System

Month	Year	Backup Location	Status	Done By	Verified By

Title: Quarterly Restore Checklist

Quarterly Restore Checklist for_____System

Backup Set	Backup Location	Status	Done By	Verified By

POLICY #12: MONTHLY BACKUP DATA SHEET	DEPARTMENT: BUSINESS INFORMATION SYSTEMS	PAGE: 7 of 7

Title: Network Checkup List

Commented [MM1]: Is it being done

Monthly checks for _____ system.

Date	Device	Log Type	Done By	Reviewed By	Comments

POLICY #12: DATA BACKUP AND RECOVERY	DEPARTMENT: BUSINESS INFORMATION SYSTEMS	PAGE: 1 of 1

Title: User Data Recovery Request Form

Full Names	
Unit	
Department	
Title	

System	
Filename	
File Date Created	
File Last Date Amended	
Reasons for the request	

Date: _____

Signature: _____

Business Information Systems Manager Signature_____

Title: Preventive Maintenance Checklist

Title:	Desktop/Laptop Maintenance		Frequency: Bi-Annually		
PC Specifications:		***Serial No.:***			
User:		***Dept.:***			
Tech:		***Date:***			
Item #	**Task**	**Description**	**OK**	**Repair**	**N/A**
1.	System Boot	Boot system from a cold start. Monitor for errors and speed of entire boot process.			
2.	System Log-in	Monitor for Errors. Monitor login script.			
3.	Network Settings	Verify the Following:			
		TCP/IP and/or IPX Settings are Correct			
		Domain Name			
		Security Settings			
		Client Configurations			
		Computer Name			
4.	Computer Hardware Settings	Verify Device Manager settings			
		BIOS up-to-date			
		Hard Disk			
		DVD or CD/RW-drive firmware up-to-date			
		Memory is O.K			
		For Laptop: battery run-time is norm			
5.	Browser/Proxy Settings	Verify proper settings and operation			
6.	Proper Software loads	Required software is installed and operating			
7.	Viruses, and malware	Anti-virus installed			
		Virus scan done			
8.	Clearance	Unused software removed			
		Temporary files removed			
		Recycle Bin and caches emptied			
		Periphery devices clean			
9.	Interiors, and cleaning	Dust removed			
		No loose parts			
		Airflow is O.K.			
		Cables unplugged and re-plugged			
		Fans are operating			

10.	Peripheral devices	Mouse			
		Keyboard			
		Monitor			
		UPS			
		Printer			
		Telephone extension			
		Fax			

NOTES

Note: To be filled by all technicians attending to ICT equipment.

RAINBOW TOURISM GROUP LTD

REMOVE USER FORM

Please remove the following associate from the RTG domain and revoke all systems access rights

1. To be completed by an HR Personnel /Line Manager			
First name:		**Initial:**	
Last name:			
SysAid / Helpdesk CR Number:			
		Date Requested:	
2. To be completed by the Systems Administrator/ IT Administrator **System Rights Revocation**			
Sage Accpac ☐	**Corporate Email** ☐	**Helpdesk System** ☐	
Opera PMS ☐	**Gateway Reporting** ☐	**VPN** ☐	
Parliamentarians ☐	**VoIP** ☐		
Materials Control ☐	**HEXA DMS** ☐		
Other ☐	**Specify** ☐		

Account Deletion Checklist

1. E-mail backup Done (Y/N) _____
2. User Files backup done (Y/N) _____
3. Active Directory Account Deleted (Y/N) _____

Signed: ....

Line Manager /HR Personnel **BIS Manager**

Implemented By: ..... **Date Implemented:** .....

Title: Add User Form

Please add the following associate as a user on the RTG domain.

First name:		**Initial:**	
Last name:			
Job Title:			
Department:			
Business Unit:			
Phone Number:			
Helpdesk CR Number:			
Signature of user:		**Date Requested:**	
Tick application access to be granted to the Associate/User			

Sage Accpac	☐	Corporate E-mail	☐	Asterisk	☐
Opera PMS	☐	VoIP	☐		
Micros POS	☐	Helpdesk System	☐		
VPN	☐	HEXA DMS	☐		
Materials Control	☐	VingCard	☐		
Parliamentarian	☐	Gateway Reporting	☐		
Other	☐ Specify				

Signed: ....

Line Manager **BIS Manager**

Implemented By: ..... **Date Implemented:** .....

Title: Acknowledgment of BIS Policy

This form is used to acknowledge receipt of and compliance with the BIS Policy.

Procedure

Complete the following steps:

1. Read the BIS Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the Human Resource Manager

Signature

By signing below, I agree to the following terms:

a) I have received and read a copy of the BIS Policy and understand and agree to the same.
b) I understand and agree that any software and hardware devices provided to me by the company remain the property of the company.
c) I understand and agree that I am not to modify, alter, or upgrade any software programs or hardware devices provided to me by the organization without the permission of the information technology department.
d) I understand and agree that I shall not copy, duplicate or allow anyone else to copy or duplicate any software.
e) I understand and agree that if I leave the company for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.
f) I understand and agree I must make reasonable efforts to protect all company-provided software and hardware devices from theft and physical damage.
g) I have read and understood the Password Policy and will abide by it.
h) I have read and understood the Email Policy and will abide by it.
i) I have read and understood the Social Media and Internet Access Policy and will abide by it.
j) I have read and understood the Software and Hardware Policy and will abide by it.
k) I have read and understood the Data Classification and Protection Policy and will abide by it.

_____ **Associate Signature**

_____ **Associate Name**

_____ **Associate Title**

_____ **Date**

_____ **Department/Location**