



# **CYBER SECURITY AND DATA PRIVACY POLICY**

# TABLE OF CONTENTS

## Contents

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>1 Introduction .....</b>                           | <b>6</b>  |
| <b>2 Information Technology security policy .....</b> | <b>6</b>  |
| 2.1 Information security requirements .....           | 6         |
| 2.2 Framework for setting objectives .....            | 6         |
| 2.3 Continual improvement of the ITS Policy .....     | 6         |
| 2.4 Information security policy areas .....           | 7         |
| 2.5 Application of information security policy .....  | 9         |
| <b>3 Internet acceptable use policy .....</b>         | <b>9</b>  |
| <b>4 Mobile device policy .....</b>                   | <b>9</b>  |
| 4.1 Devices provided by Rolex Rings .....             | 9         |
| <b>5 HR security policy .....</b>                     | <b>10</b> |
| 5.1 Prior to employment .....                         | 10        |
| 5.1.1 Background checks .....                         | 10        |
| 5.1.2 Employment contracts .....                      | 10        |
| 5.2 During employment .....                           | 10        |
| 5.2.1 Management responsibilities .....               | 10        |
| 5.2.2 Information security awareness .....            | 10        |
| 5.2.3 Disciplinary process .....                      | 11        |
| 5.3 Termination and change of employment .....        | 11        |
| 5.3.1 Change of role .....                            | 11        |
| 5.3.2 Termination .....                               | 11        |
| <b>6 Acceptable use policy .....</b>                  | <b>11</b> |
| 6.1 Desktop/ Laptop Usage .....                       | 11        |
| 6.2 Access control .....                              | 12        |
| 6.3 Data/Privacy protection .....                     | 12        |
| 6.4 Email access .....                                | 13        |
| 6.5 Virus protection .....                            | 14        |
| 6.6 Reporting security incidents/ weaknesses .....    | 14        |
| <b>7 Asset management policy .....</b>                | <b>15</b> |
| 7.1 Responsibility for assets .....                   | 15        |
| 7.2 Information classification .....                  | 15        |
| 7.3 Media handling .....                              | 17        |
| <b>8 Access Control Policy .....</b>                  | <b>17</b> |
| 8.1 Business requirements of access control .....     | 17        |
| 8.2 User access management .....                      | 17        |
| 8.2.1 User registration and de-registration .....     | 17        |
| 8.2.2 User access provisioning .....                  | 18        |
| 8.2.3 Removal or adjustment of access rights .....    | 18        |
| 8.2.4 Management of privileged access rights .....    | 19        |

|                                                          |           |
|----------------------------------------------------------|-----------|
| 8.2.5 User authentication for external connections ..... | 19        |
| 8.2.6 Review of user access rights.....                  | 19        |
| 8.2.7 User authentication and password policy .....      | 19        |
| <b>8.3 User responsibilities .....</b>                   | <b>20</b> |
| <b>8.4 System and application access control.....</b>    | <b>21</b> |
| <b>9 Physical Security Policy .....</b>                  | <b>21</b> |
| 9.1 Secure areas .....                                   | 21        |
| 9.2 Paper and equipment security.....                    | 21        |
| 9.3 Equipment life-cycle management .....                | 22        |
| <b>10 Clear desk and clear screen policy.....</b>        | <b>22</b> |
| <b>11 Cryptographic Policy .....</b>                     | <b>23</b> |
| 11.1 Policy on the use of Cryptographic controls .....   | 23        |
| 11.1.1 Risk assessment .....                             | 23        |
| 11.1.2 Technique selection .....                         | 23        |
| 11.1.3 Deployment .....                                  | 24        |
| 11.1.4 Testing and review .....                          | 24        |
| 11.2 Key management .....                                | 24        |
| <b>12 Anti-malware policy.....</b>                       | <b>24</b> |
| 12.1 The malware threats .....                           | 24        |
| 12.1.1 Definition .....                                  | 24        |
| 12.2 Anti-malware policy .....                           | 24        |
| 12.2.1 Firewall .....                                    | 25        |
| 12.2.2 Anti-virus .....                                  | 25        |
| 12.2.3 Spam filtering.....                               | 25        |
| 12.2.4 Software installation and scanning .....          | 25        |
| 12.2.5 Vulnerability management.....                     | 25        |
| 12.2.6 User awareness training.....                      | 25        |
| 12.2.7 Threat monitoring and alerts .....                | 25        |
| 12.2.8 Technical reviews .....                           | 26        |
| 12.2.9 Malware incident management .....                 | 26        |
| <b>13 Backup Policy.....</b>                             | <b>26</b> |
| 13.1 Backup logging and audit trail .....                | 27        |
| 13.2 Backup Storage.....                                 | 27        |
| <b>14 Logging and monitoring policy .....</b>            | <b>27</b> |
| 14.1 Audit logging .....                                 | 27        |
| 14.2 Monitoring system use .....                         | 28        |
| 14.3 Protection of log information .....                 | 28        |
| 14.4 Administrator and operator logs.....                | 28        |
| 14.5 Fault logging.....                                  | 28        |
| 14.6 Clock synchronization.....                          | 29        |
| <b>15 Software Policy .....</b>                          | <b>29</b> |
| 15.1 Use of software on-premises .....                   | 29        |
| 15.1.1 Purchasing software.....                          | 29        |
| 15.1.2 Software Registration .....                       | 29        |
| 15.1.3 Software Installation .....                       | 29        |

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| 15.1.4 Removal of software .....                                        | 30        |
| 15.1.5 In-house software development .....                              | 30        |
| <b>16 Technical vulnerability management policy .....</b>               | <b>30</b> |
| 16.1 What is a technical vulnerability? .....                           | 30        |
| 16.2 Sources of information .....                                       | 30        |
| 16.3 Patches and updates .....                                          | 31        |
| 16.4 Vulnerability assessment .....                                     | 31        |
| 16.5 Awareness training .....                                           | 31        |
| <b>17 Change Management Policy .....</b>                                | <b>31</b> |
| <b>18 Email Security policy .....</b>                                   | <b>32</b> |
| 18.1 Sending and receiving electronic messages .....                    | 32        |
| 18.2 Monitoring of Email facilities .....                               | 33        |
| 18.3 Use of email .....                                                 | 33        |
| <b>19 System Acquisition, Development, and Maintenance Policy .....</b> | <b>34</b> |
| 19.1 Security requirements of information systems .....                 | 34        |
| 19.2 Security in development and support processes .....                | 35        |
| 19.2.1 Secure development .....                                         | 35        |
| 19.2.2 Acceptance Testing .....                                         | 35        |
| 19.2.3 Test data .....                                                  | 36        |
| <b>20 Information security policy for supplier relationships .....</b>  | <b>36</b> |
| 20.1 General provisions .....                                           | 36        |
| 20.2 Addressing security within supplier agreements .....               | 36        |
| 20.3 Evaluation of existing suppliers .....                             | 37        |
| 20.4 Managing changes to supplier services .....                        | 37        |
| 20.4.1 Changes within contract .....                                    | 37        |
| 20.4.2 Contractual Disputes and end of contracts .....                  | 37        |
| 20.4.3 Exception .....                                                  | 37        |
| <b>21 Incident Management Policy .....</b>                              | <b>37</b> |
| 21.1 Policy statement .....                                             | 37        |
| 21.2 Policy Details .....                                               | 37        |
| 21.2.1 Incident Management .....                                        | 37        |
| 21.2.2 Reporting information security events and weakness .....         | 38        |
| 21.2.3 Collection of evidences .....                                    | 38        |
| 21.2.4 Annexure .....                                                   | 38        |
| <b>22 Availability management policy .....</b>                          | <b>39</b> |
| 22.1 Availability monitoring and reporting .....                        | 39        |
| 22.2 Non-availability .....                                             | 39        |
| 22.2.1 Planned .....                                                    | 39        |
| 22.2.2 Unplanned .....                                                  | 40        |
| 22.3 Availability plan testing .....                                    | 40        |
| 22.4 Impact of changes .....                                            | 40        |
| <b>23 Records retention and protection policy .....</b>                 | <b>40</b> |

|                                                             |           |
|-------------------------------------------------------------|-----------|
| 23.1 General principles .....                               | 40        |
| 23.2 Record types and guidelines .....                      | 40        |
| 23.3 Use of cryptography .....                              | 40        |
| 23.4 Record retrieval.....                                  | 40        |
| 23.5 Record destruction .....                               | 41        |
| 23.6 Record review .....                                    | 41        |
| <b>24 Privacy and personal data protection policy .....</b> | <b>41</b> |
| 24.1 Privacy by design .....                                | 41        |
| 24.2 Breach notification .....                              | 41        |
| <b>25 Internal Audit Policy .....</b>                       | <b>41</b> |
| <b>26 Network security policy .....</b>                     | <b>42</b> |
| <b>26.1 Network security design .....</b>                   | <b>42</b> |
| 26.1.1 Requirements .....                                   | 42        |
| 26.1.2 Defence in depth.....                                | 42        |
| 26.1.3 Network segregation.....                             | 43        |
| 26.1.4 Perimeter security.....                              | 43        |
| 26.1.5 Public networks.....                                 | 43        |
| 26.1.6 Wireless networks.....                               | 43        |
| 26.1.7 Physical security.....                               | 43        |
| 26.1.8 Remote access .....                                  | 44        |
| 26.1.9 Network intrusion detection .....                    | 44        |
| 26.1.10 Network security standards .....                    | 44        |
| 26.1.11 Network hardware.....                               | 44        |
| 26.1.12 IP addressing.....                                  | 44        |
| 26.1.13 Network protocols .....                             | 44        |
| <b>26.2 Network security management .....</b>               | <b>45</b> |
| 26.2.1 Roles and responsibilities .....                     | 45        |
| 26.2.2 Logging and monitoring .....                         | 45        |
| 26.2.3 Network changes .....                                | 46        |
| 26.2.4 Network security incidents.....                      | 46        |
| <b>27 Cloud Security Policy .....</b>                       | <b>46</b> |

## 1 Introduction

This document defines the information security policy of Rolex Rings Private Limited (Hereafter referred to as 'Rolex Rings').

Rolex Rings recognizes at senior levels the need to ensure that its operations run smoothly and without interruption for the benefit of its users and stakeholders.

In order to provide such a level of continuous operation, Rolex Rings has implemented an Information Technology Security Policy.

The operation of the ITS Policy has many benefits for Rolex Rings, including:

- Continual improvement the level of security to all it's information
- Enhancing defence against Cyber attacks
- Cost optimization
- Safeguarding confidentiality, integrity and availability of data.
- Centrally managed security

This policy applies to all employees of Rolex Rings and any supplier / contractor / third party who affects the information security of Rolex Rings in any way.

## 2 Information Technology security policy

### 2.1 Information security requirements

A clear definition of the requirements for information security within Rolex Rings will be agreed and maintained with the internal team and the relevant stakeholders. Statutory, regulatory and contractual requirements will also be documented and will be used as an input to the planning process.

It is a fundamental principle of the Rolex Rings' s Information Technology Security Policy that the controls implemented are driven as per the security requirement and this will be regularly communicated to all relevant stakeholders.

### 2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security. This will ensure that adequate funding is obtained for the improvement of the activities identified. These objectives will be based upon results of security requirements and continual improvement, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

### 2.3 Continual improvement of the ITS Policy

Rolex Rings policy regarding continual improvement is to:

- Continually improve the effectiveness of the IT Security
- Increase the level of pro activity with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions

- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties
- Review ideas for improvement at regular management meetings in order to prioritize and assess timescales and benefits

Ideas for improvements may be obtained from source including but not limited to employees, stakeholders, third party, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

## 2.4 Information security policy areas

Rolex Rings defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, Rolex Rings.

The table below shows the individual policies within the documentation set and summarizes each policy's content and the target audience of interested parties.

| POLICY TITLE                   | AREAS ADDRESSED                                                                                                                                                                                                | TARGET AUDIENCE              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Internet Acceptable Use Policy | Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.                                                  | All employees of Rolex Rings |
| Mobile Device Policy           | Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by Rolex Rings or the individual for business use.                                                              | All employees of Rolex Rings |
| Teleworking Policy             | Information security considerations in establishing and running a teleworking site and arrangement                                                                                                             | All employees of Rolex Rings |
| Access Control Policy          | User registration and de-registration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.                          | All employees of Rolex Rings |
| Cryptographic Policy           | Risk assessment, technique selection, deployment, testing and review of cryptography, and key management                                                                                                       | All employees of Rolex Rings |
| Anti-Malware Policy            | Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management. | All employees of Rolex Rings |
| Backup Policy                  | Backup cycles, backup storage, documentation, recovery, testing and protection of storage                                                                                                                      | All employees of Rolex Rings |
| Logging and                    | Settings for event collection, protection and                                                                                                                                                                  | All employees of Rolex       |

Policy Adopted on May, 25, 2023

| POLICY TITLE                                           | AREAS ADDRESSED                                                                                                                                        | TARGET AUDIENCE              |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Monitoring Policy                                      | review                                                                                                                                                 | Rings                        |
| Software Policy                                        | Purchasing software, software registration, installation and removal, in-house software development.                                                   | All employees of Rolex Rings |
| Technical Vulnerability Management Policy              | Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.                     | All employees of Rolex Rings |
| Electronic Messaging Policy                            | Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.                                             | All employees of Rolex Rings |
| Information Security Policy for Supplier Relationships | Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.                                          | All employees of Rolex Rings |
| Availability Management Policy                         | Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.                     | All employees of Rolex Rings |
| Records Retention and Protection Policy                | Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.                            | All employees of Rolex Rings |
| Privacy and Personal Data Protection Policy            | Applicable data protection legislation, definitions and requirements.                                                                                  | All employees of Rolex Rings |
| Incident Management Policy                             | Incident Identification, Reporting Information Security Events and Weakness, Learning from Information security Incidents and Collection of Evidences. | All employees of Rolex Rings |
| Change Management Policy                               | Change Management process, Change approval, Changes and Backup, Emergency Changes                                                                      | All employees of Rolex Rings |
| HR Security Policy                                     | Recruitment, employment contracts, policy compliance, disciplinary process, termination                                                                | All employees of Rolex Rings |
| Acceptable Use Policy                                  | Employee commitment to organizational information security policies                                                                                    | All employees of Rolex Rings |
| Asset Management Policy                                | This document sets out the rules for how assets must be managed from an information security perspective.                                              | All employees of Rolex Rings |
| Physical Security Policy                               | Sets out the rules about the protection of physical infrastructure from threats                                                                        | All employees of Rolex Rings |

Table 1: Set of policy documents

## 2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Rolex Rings and must be complied with. Failure by an employee/third-party to comply with these policies may result in disciplinary action being taken in accordance with Rolex Rings's Employee Disciplinary Process.

Questions regarding any Rolex Rings policy should be addressed in the first instance to the employee's reporting manager or can be emailed at [infosec@rolexringsltd.com](mailto:infosec@rolexringsltd.com) or [itsupport@rolexringsltd.com](mailto:itsupport@rolexringsltd.com)

## 3 Internet acceptable use policy

Rolex Rings allows users to use LAN/WiFi based internet within Rolex Rings premises and access information through data card provisioned by Rolex Rings HR department.

As per Internet acceptable use policy internet access must be used in accordance with this policy for tasks reasonably related to your work including:

- Access to information and systems that is pertinent to fulfilling Rolex Rings's business requirements obligations
- The capability to post updates to organization-owned and/or maintained web sites and social media accounts
- An electronic commerce facility (e.g., purchasing equipment for Rolex Rings)
- Research related to business needs

## 4 Mobile device policy

### 4.1 Devices provided by Rolex Rings

- Unless specifically authorized, only mobile devices (laptop or any movable device used for data center operations purpose) provided by Rolex Rings must be used to hold or process classified information on behalf of Rolex Rings .
- If you are required to make use of mobile equipment, you will be provided with an appropriate device(s) which will be configured to comply with Rolex Rings' Policies. Support will be provided by the IT Team who may at times need access to your device for problem resolution and maintenance purposes.
- You must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged.
- Do not leave the device unattended in public view
- Do not remove any identifying marks on the device such as a company asset tag or serial number. Ensure that the device is locked away when being stored and that the key is not easily accessible.
- Do not add peripheral hardware to the device without the approval of the IT Infrastructure Head. This is to ensure that it will work and to consider any insurance implications.
- You will not hold classified information on the device unless this has been authorized and appropriate controls (e.g., encryption) put in place. Do not keep access tokens, Personal Identification Numbers or other security items with the device.
- Ensure that the device screen locks after a short period of not being used and requires an access code or password to unlock it. Passwords used must be strong and difficult to guess. No unsecured logons (i.e., those that do not require a password) may be set up on the device.

- Rolex Rings -provided device is for your business use only; it must not be shared with family or friends or used for personal activities. You may be asked to return the device to the IT Support at any time for inspection and audit. You must not install any unauthorized software or change the configuration or setup of the device without consulting the IT Support first.
- Where applicable, virus protection will be installed on the device by Rolex Rings . Ensure that the device is connected to the internet on a regular basis to allow the virus signatures to be updated. Do not disable virus protection on the device.

## 5 HR security policy

### 5.1 Prior to employment

#### 5.1.1 Background checks

Appropriate background verification checks will be carried out via authorized third-party considering the applicable legislation/regulations on all candidates for employment prior to their starting work with Rolex Rings.

The specific screening activities that should be applied in any particular case will depend on a number of risk factors including, but not limited to, the following:

- The classification of information they will have access to
- If the role will have access to financial assets
- The level of potential to cause harm to Rolex Rings
- Level of involvement in technology
- Any other factors that are deemed by management to be relevant to the ongoing security of Rolex Rings

A judgement must be made in each case about the appropriate level of background verification to be applied. This must reach a balance between being sufficiently rigorous to protect Rolex Rings without placing an undue burden of time, cost or effort on the recruitment process.

#### 5.1.2 Employment contracts

Employment contracts, including those with contract staff, must specify relevant requirements for information security, including a commitment to comply with Rolex Rings Limited policies in this area. Roles that have access to classified information will also be required to sign a Non-Disclosure Agreement (NDA).

### 5.2 During employment

#### 5.2.1 Management responsibilities

It is important that all employees with management responsibility ensure that Rolex Rings information security-related policies and procedures are followed by staff (both internal employees and users) within their supervision at all times. Any instances of non-compliance must be identified and addressed through normal management channels, including disciplinary action where appropriate.

#### 5.2.2 Information security awareness

Information security awareness training will be provided to all IT employees and contractors to a level of detail appropriate to their job role. This will include information about Rolex Rings policies and procedures and the specific risks and threats relevant to the employee or contractor's area of work.

Awareness training will be delivered as part of new starter inductions and updates to relevant information communicated to all employees and contractors when appropriate, and in a timely manner, at least once in a year to the existing employees

### 5.2.3 Disciplinary process

Instances where a clear breach of information security policy or procedure has been committed by an employee will be subject to Rolex Rings disciplinary procedures. In serious cases, where Rolex Rings has been put at significant risk as a result of the employee's actions, termination of employment may be considered. Disciplinary process should not start without prior verification that an information security breach has occurred.

In less serious cases, the provision of additional information security awareness training may be appropriate as one of the actions to address the situation.

## 5.3 Termination and change of employment

### 5.3.1 Change of role

In situations where an employee experiences a temporary or permanent change of job role, including reassignment, secondment and sabbatical, those information security responsibilities from their previous role (for example for confidentiality) that will continue must be defined and emphasized to the employee.

Any failure on the part of the employee to observe their continuing responsibilities for information security may be subject to disciplinary action.

### 5.3.2 Termination

Where an employee's position with Rolex Rings is terminated on a permanent basis, the information security responsibilities and duties that must continue to be observed post-employment will be defined in writing and communicated to the employee.

It must be stated to the terminated employee that any failure on their part to observe their continuing responsibilities for information security may be subject to legal action.

## 6 Acceptable use policy

### 6.1 Desktop/ Laptop Usage

#### **Acceptable Usage:**

- Desktops/ laptops provided to employees shall be used only for official purpose
- Users shall only use Rolex Rings approved application/software
- Users shall always keep their desktop/ laptop suitably fastened/ locked. Adequate precautions should also be taken to ensure safe carriage of laptops during travel.
- In the event of a laptop being stolen, the concerned personnel shall file a police report and subsequently inform the administration department.
- Users using external internet connections on laptops shall ensure that:
  - Anti-virus signatures are updated
  - Latest security patches are installed
- Classified data shall not be copied to external portable media like USBs, CDs, etc. without

the permission of the IT Head.

- All sensitive information on laptop should be secured through password.

**Unacceptable Usage:**

- Users shall not install freeware or shareware which are not provided/authorized by Rolex Rings
- Users shall not use external devices unless it is approved

## 6.2 Access control

**Acceptable Usage:**

- All Rolex Rings Users shall use their unique ID assigned to them for accessing Rolex Rings information assets
- All Rolex Rings employees shall adhere to the password policies of Rolex Rings as listed below:-
  - Passwords should have a minimum length of eight (8) characters
  - Password should have alpha numeric and special characters
  - Passwords of Rolex Rings users should be changed once in 60 days
- All Rolex Rings users shall change their password every 60 days or before. While some applications will enforce password change and complexity on users automatically, it may not be feasible to enforce it for all accounts and for all applications. Users must change their passwords under any of the following circumstances
  - At least once in 60 days.
  - As enforced by system (applications and operating system)
  - As soon as possible, after you suspect that a password has been compromised.

**Unacceptable Usage:**

- Users shall not use shared accounts for accessing Rolex Rings information assets unless approved by IT head
- Users shall not share their passwords with anyone
- Users shall not write or paste passwords in public spaces or at the workplace
  - Last 5 passwords shall not be used and this shall be controlled by technical means such as password history. This applies to domain controller.
  - User name shall not be used as a password
  - Passwords shall not be stored and transmitted in clear text on computer system and shall be stored in an encrypted format.
  - Passwords shall not be stored in reversible encryption

## 6.3 Data/Privacy protection

**Acceptable Usage:**

Policy Adopted on May, 25, 2023

- Users shall understand business/ contractual requirements of data protection from their respective managers or Top Management.
- Users shall ensure protection of information assets as per the classification
- Users shall protect vital physical records which contain business related information
- Users shall store their work files on the assigned folder to them, from which IT team can take a backup

**Unacceptable Usage:**

- Users shall not send business data to any unauthorized third party
- Users shall not use their mobile phones for capturing photos/videos of business information without authorization.
- Users shall not leave confidential documents on the desk; instead it should be kept in a locked cabinet
- Users shall not leave printouts unattended at the printer machine
- Users shall not reveal information about Rolex Rings business details in white papers or presentations
- Users shall not discuss official matters in public places

#### 6.4 [Email access](#)

**Acceptable Usage:**

- Users shall use Rolex Rings e-mail only for official purposes
- Users shall exercise caution in disclosing Rolex Rings e-mail address to strangers
- Users shall be cautious in opening attachments from suspicious e-mail addresses. Be particularly suspicious of files that have suffixes such as .jpg.vbs, .txt.shs, .pif, .exe, .shs, .vbs, .chm, .com, .scr, .hta, .hto, .dll and .bat, mp3,.ace, .ani, .app, .docm, .jar, .reg, .scr, .vbe, .bat, .cer, .cmd, .hlp, .js, .pst, .tmp, .url,.wsf, .htm, .html
- Users shall report suspicious e-mails to IT team on infosec@Rolex Rings Ltd.com
- Users shall archive mails and take regular backups
- Users shall follow the controls specified by Rolex Rings while accessing emails from mobiles/ PDAs
- Users shall report about spam to IT team on infosec@Rolex Rings Ltd.com
- Users shall protect their e-mail account through strong password and should not share their password or account with anyone else.

**Unacceptable Usage:**

- Users shall not use e-mails within Rolex Rings to harass other users
- Users shall not send unwanted e-mails to the outside world that project a wrong image of Rolex Rings
- Users shall not communicate with any third party which may potentially invite involvement

of law enforcement agencies

- Users shall not participate in spam chain e-mails
- Users shall not forward sensitive e-mails containing Rolex Rings information to the external world, even inadvertently
- Users shall not register Rolex Rings e-mail addresses on external websites without authorization
- Users shall not respond to spam mails as it can make user accounts potential target for spammers.
- Users shall not click on links provided in e-mails that ask for personal information against your account (e.g., bank account user-id and password details). These mails are largely phishing attacks carried out by hackers.
- Users shall not share sensitive information like credit card no, account details etc. over the e-mail.

## 6.5 Virus protection

### **Acceptable Usage:**

- Users should ensure that anti-virus agent is installed with latest signatures on the desktop/laptop
- Users shall promptly communicate to their immediate supervisor/ senior and IT Team, if they discover any security incident (like virus infection, unusual activity, passwords shared etc.)

### **Unacceptable Usage:**

- Users shall not open attachments from unknown sources
- Users shall not use any external source such as CDs; USB drives etc. on Rolex Rings infrastructure unless scanned for viruses, and approved by the management.

## 6.6 Reporting security incidents/ weaknesses

- It is the responsibility of each employee to report any observed or suspected information security incidents and/or weaknesses to the help desk on telephone and by email to [infosec@RolexRingsLtd.com](mailto:infosec@RolexRingsLtd.com)
- Users shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness shall be interpreted as a potential misuse of the system.
- Users shall not discuss with colleagues about the suspected weakness once it is reported to higher authority for investigation.

## 7 Asset management policy

### 7.1 Responsibility for assets

An inventory of assets associated with information and information processing facilities within Rolex Rings will be maintained with owner and criticality. The types of assets to be identified and controlled will include:

- Hard Information Assets
- Soft Information Assets
- Physical Assets
- People Assets
- Software Assets

Users will need to sign the [Acceptable use policy - Signed Template](#)

Each asset recorded in the inventory will be assigned an agreed owner who will ensure that:

- All assets under their ownership are included in the inventory
- An appropriate classification is assigned to the assets
- Access to the assets is controlled appropriately
- Assets are handled correctly, including their disposal

The asset owner should be a role such as IT head. Day to day operation and maintenance of the asset may be delegated by the owner to a custodian. Rules for the secure use of the assets will be defined by the owner and communicated to those who have access to them.

Upon termination of employment, resignation, retirement, or death of employee, all assets that have been issued to the terminated party must be returned to local HR person and a no-due certificate shall be taken before the final settlement of dues from HR, including the secure removal of organization data from personal equipment. The local HR person will hand over assets to IT in case of HO and Plants where IT persons are deputed. In case of death of an employee, local HR / Head office HR team will coordinate with deceased employee's family member and collect asset based on comfortable time/date with family members and collect assets.

In case of remote locations where IT persons are not deputed, local HR will recover asset and keep in their custody. They will inform IT team of the same to update IT records. If recovered asset is to be allocated to another employee in future, same will be informed to IT team and based on HR communication, the asset will be allocated to another employee in IT records

### 7.2 Information classification

All information within Rolex Rings will be subject to security classification. The information classification scheme requires information assets to be protectively marked as one of four classifications (excluding Public information which does not need to be marked). The way the information is handled, published, moved and stored will be dependent on this scheme.

The classes of information in Rolex Rings are:

Level 1: Public

Level 2: Protected

Level 3: Restricted

Level 4: Confidential

| Classification Level | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CONFIDENTIAL         | <p>This classification applies to sensitive business information, which is intended for use within Rolex Rings. Its unauthorized disclosure could adversely impact the organization, its stockholders, its business partners, its employees, and/or its customers. Information that some people would consider to be private is included in this classification.</p> <p>Information must be classified as CONFIDENTIAL if it meets any of the following criteria:</p> <p>Proprietary information of Rolex Rings, which can be shared only among a few individuals, on a need to know basis.</p> <p>Information of parties external to Rolex Rings for example Customers, Prospects, Vendors, Partners, etc., which can be shared only among a few individuals on a need to know basis.</p> <p>All project related information that is covered under an NDA (non-disclosure agreement)</p> |
| RESTRICTED           | <p>Information must be classified as RESTRICTED if it meets any of the following criteria and is not classified as CONFIDENTIAL:</p> <p>Proprietary information of Rolex Rings, which can be shared among the relevant function/s or project execution group/s.</p> <p>Information of parties external to Rolex Rings which can be shared among the relevant Function/s or project execution groups</p> <p>HR information about employee</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PROTECTED            | <p>This classification applies to all other information, which does not clearly fit into any of the other three classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the organization, its employees, its stockholders, its business partners, and/or its customers. Such includes internal use documents which are meant to be shared within Rolex Rings .</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|        |                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUBLIC | This classification applies to information, which has been explicitly approved by Rolex Rings management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The decision regarding which classification an information asset should fall into will be based on the following main criteria:

1. Legal requirements that must be complied with
2. Value to Rolex Rings
3. Criticality to Rolex Rings
4. Sensitivity to unauthorized disclosure or modification

All classified information must be clearly labeled with the classification that has been assigned, so that employees, customers and third parties are aware of the level of protection that must be applied, in accordance with Rolex Rings procedures.

### 7.3 Media handling

Removable media (for example USB drives, memory stick or other removable devices) must not be used to store classified information unless its use is authorized by the IT Head.

Employees and contractors must not save organization data to memory stick, USB drives, or other removable media as backups, to take data to a third-party site, without the prior approval of the IT Head.

Rolex Rings uses removable media for only for business purpose. Removable media is included in the inventory as other assets.

## 8 Access Control Policy

### 8.1 Business requirements of access control

Business requirements for access control must be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design. Access to Rolex Rings information systems will be given based on need to know basis.

### 8.2 User access management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. They must cover all stages of the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

#### 8.2.1 User registration and de-registration

A request for access to Rolex Rings' network and computer systems must first be submitted to the IT Team for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorization is obtained prior to user

account creation. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique username that is not shared with any other user and is associated with a specific individual i.e., not a role or job title. Generic user accounts i.e., single accounts to be used by a group of people must not be created as they provide insufficient allocation of responsibility. Exception shall be given to generic IDs based on formal HR head and application head approval.

An initial strong password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves Rolex Rings under normal circumstances, their access to all data must be suspended at the close of business on the employee's last working day. It is the responsibility of the HR team to request the suspension of the access rights.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm Rolex Rings prior to or upon termination, a request to remove access may be approved and be actioned in advance of notice of termination being given. This precaution will especially apply in the case where the individual concerned has privileged access rights e.g., domain admin.

User accounts must be initially suspended or disabled only and not deleted. User account names must not be reused as this may cause confusion in the event of a later investigation.

#### 8.2.2 User access provisioning

Each user must be allocated access rights and permissions to services and data that are commensurate with the tasks they are expected to perform. In general, this will be role-based i.e., a user account will be added to a group that has been created with the access permissions required by that job role.

Roles must be maintained in line with business requirements and any changes to them must be formally authorized and controlled via the change management process.

Ad hoc additional permissions must not be granted to user accounts outside of the group role; if such permissions are required this must be addressed as a change and formally requested.

The unique ID (employee ID) for new employees shall be assigned by the Human Resource (HR) Department. Intimation mail shall be sent to HR team upon creation of a new employee ID. The HR Department shall request IT Department to create and deactivate the domain access and e-mail ID based on business requirement / applicability.

#### 8.2.3 Removal or adjustment of access rights

Where an adjustment of access rights or permissions is required e.g., due to an individual changing role, this must be carried out as part of the role change. It must be ensured that access rights no longer required as part of the new role are removed from the user account. If a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role must be requested via change management. Due consideration of any issues of segregation of duties must be given.

Under no circumstances will administrators be permitted to change their own user accounts or permissions.

Policy Adopted on May, 25, 2023

#### 8.2.4 Management of privileged access rights

The privileged accounts associated with each type of information systems such as operating system, business applications, databases and network devices (e.g. switches, routers etc.) shall be restricted, identified, reviewed, controlled and documented. Generic admin accounts must not be used as they provide insufficient identification of the user.

Access to admin level permissions must only be allocated to individuals whose roles require them and who have received enough training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs must be avoided where possible. Where this is unavoidable the password used must be protected and changed on a regular basis.

The accounts with “administrator” or “super user” capabilities would be defined as privileged accounts or accounts with privileged access rights.

- Privileges access rights shall not be granted until authorization process is complete
- Privileged access shall be granted as per job responsibilities and on the principles of “need-to-use” basis with appropriate authorization
- Sharing of privileged user IDs shall be prohibited and user IDs shall be unique in nature.
- Access review for privileged user IDs must be performed at least once in six months for critical business applications, operating system, database and network devices

#### 8.2.5 User authentication for external connections

Rolex Rings allow their employees to access the business systems from external connection and the involved risks are highlighted in risk register which shall be accepted by Rolex Rings .

For further information please refer to the Mobile Device Policy and Teleworking Policy.

#### 8.2.6 Review of user access rights

IT Application and Infrastructure Head must review who has access to their areas of responsibility and the level of access in place once in a year. This will be to identify:

- People who should not have access (e.g. leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification, e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by the IT Head every six months to ensure that this policy is being complied with.

#### 8.2.7 User authentication and password policy

Rolex Rings ’s policy is to make use of additional authentication methods based on a risk assessment which takes into account:

Policy Adopted on May, 25, 2023

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Use of multi-factor authentication methods must be justified based on the above factors and securely implemented and maintained where appropriate.

Whether single or multi-factor authentication is used, the quality of user passwords must be enforced in all networks and systems using the following parameters:

| PARAMETER              | VALUE                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Minimum length         | 8                                                                                                                         |
| Maximum length         | As per the system capabilities                                                                                            |
| Re-use cycle           | Cannot be the same as any of the previous 5 passwords                                                                     |
| Characters Required    | At least one upper-case letter<br>At least one lower-case letter<br>At least one special character<br>At least one number |
| Change Frequency       | At least every 60 days                                                                                                    |
| Account lockout        | On 5 incorrect logon attempts                                                                                             |
| Account lockout action | Account must be re-enabled by technical team based on request and approval                                                |
| Other controls         | Password cannot contain the user name<br>Password must not be on a list of common passwords e.g. Password1                |

Table 2: Passwords policy

### 8.3 User responsibilities

In order to exercise due care and try to ensure the security of its information, Rolex Rings expends a significant amount of time and money in implementing effective controls to reduce risk and vulnerabilities.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm Rolex Rings.

In order to maximize the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out as per the password policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically e.g. in a file or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out
- Leave nothing clearly visible that may contain access information such as login names and passwords
- Inform the CISO of any changes to their role and access requirements

Policy Adopted on May, 25, 2023

Failure to comply with these requirements may result in Rolex Rings taking disciplinary action against the individual(s) concerned.

#### 8.4 System and application access control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control must be addressed and appropriate measures implemented.

These must consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups) based on user's job responsibilities
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
  - Non-display of password as it is entered
  - Account lockout once number of incorrect logon attempts exceeds a specified threshold
  - Provide information about number of unsuccessful logon attempts and last successful logon once user has successfully logged on
  - Date and time-based logon restrictions
  - Device and location logon restrictions
- User inactivity timeout
- Password management, including
  - Ability for user to change password
  - Controls over acceptable passwords
  - Password expiry
  - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Where we spoke software development is undertaken, program source code must be protected from unauthorized access in accordance with the document Secure Development Environment Guidelines.

Access to privileged utility programs that provide a method of bypassing system security (e.g., data manipulation tools) must be strictly controlled and their use restricted to identified individuals and specific circumstances e.g., as part of a named project or change.

### 9 Physical Security Policy

#### 9.1 Secure areas

Sensitive information must be stored securely. A risk assessment must be conducted to identify the appropriate level of protection to be implemented to secure the information being stored.

#### 9.2 Paper and equipment security

Paper based (or similar non-electronic) information must be assigned an owner and a classification. Appropriate information security controls must be put in place to protect it according to the provisions in the Asset Handling Procedure.

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration
- Limit the risk of theft – e.g. if necessary, items such as laptops should be physically attached to the desk
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorized people

Data must be stored on network file servers where available. This ensures that information lost, stolen or damaged via unauthorized access can be restored and its integrity maintained.

All Rolex Rings equipment should be uniquely identifiable.

### 9.3 Equipment life-cycle management

Staff involved with maintenance must:

- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorized technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

The use of equipment off-site must be formally approved by the IT Infrastructure Head.

Information security arrangements must be subject to regular independent audit and security improvements recommended where necessary.

## 10 Clear desk and clear screen policy

This policy applies to information that has been defined as Internal, Confidential and Restricted in accordance with Rolex Rings Information Classification Procedure.

The following actions must be taken to ensure the security of information displayed on a computer or device screen:

- Screens must be locked when unattended, so that classified information is not displayed, and no access is available to restricted systems
- Screen locks must be protected by a password (or other approved mechanism) that meets organization policies on strength
- Care must be taken that screens are not sited such that the information displayed on them can be easily seen by unauthorized people
- Users must remain aware of situations in which their screen may be overlooked by unauthorized people, including visitors
- Cameras or other recording devices must not be used in the vicinity of screens which may display classified information

Creation and handling of printed materials containing classified information must conform to the following controls:

- Where possible, the printing of classified information must be avoided
- When classified information is printed, care must be taken that printouts are not accessible to unauthorized people
- When unattended, classified printed information must be locked away and appropriate control exercised over the key or other security mechanism

Policy Adopted on May, 25, 2023

- Classified printed materials must not be left on desks (or other unsecured areas).
- Use of photocopiers must be subject to access controls to prevent their use by unauthorized people

In addition to the above, care must also be taken over classified information that may be displayed on other media, such as whiteboards, flip charts and sticky notes. These must be wiped or removed after use so that the classified information is no longer displayed.

## 11 Cryptographic Policy

### 11.1 Policy on the use of Cryptographic controls

In order to identify those areas in which the deployment of Cryptographic techniques will be useful, Rolex Rings will take a managed approach as follows.

#### 11.1.1 Risk assessment

The first step will be to undertake a risk assessment in line with the ISO/IEC 27001 Information Security standard. For each of the information assets identified within Rolex Rings, possible threats will be assessed together with their likelihood and impact should they occur.

The following documents within the Rolex Rings Information Security Management System set out how this is achieved:

- Risk Assessment Sheet

#### 11.1.2 Technique selection

Once the general need for the use of cryptography has been identified by the risk assessment, a decision needs to be made about which specific techniques will be deployed.

Note that the selection of such techniques must take into account any current regulations, statutory requirement or national restrictions on the procurement and use of Cryptographic technology.

These may affect the type, strength and quality of the encryption algorithm used.

In general, the policy of Rolex Rings is to use the following techniques for the relevant business process or situation:

| PROCESS/SITUATION                  | TECHNIQUE                                    | SPECIFIC GUIDANCE                                                                      |
|------------------------------------|----------------------------------------------|----------------------------------------------------------------------------------------|
| Protection of passwords on systems | All passwords must be hashed                 | SHA-1 and SHA-2 to be used                                                             |
| Email Security                     | Symmetric/asymmetric encryption using S/MIME | Features available in the relevant email client should be used to simplify the process |
| Server and Website Encryption      | 2048 Bit RSA Certificate                     |                                                                                        |
| VPN                                | Diffie-Hellman                               | 5140 bits                                                                              |

Table 3: Cryptographic techniques

The continued use of the specified techniques will be evaluated on each review of this policy.

#### 11.1.3 Deployment

The deployment of Cryptographic techniques must be managed carefully to ensure that the desired level of security is in fact achieved.

#### 11.1.4 Testing and review

The results of VAPT should show if there are any unapproved and vulnerable Cryptographic algorithms

### 11.2 Key management

Rolex Rings is not sending any type of classified information over the public network to unauthorized individuals or organizations. Key is stored within Rolex Rings wherever feasible.

## 12 Anti-malware policy

### 12.1 The malware threats

#### 12.1.1 Definition

“Malware is any code or software that may be harmful or destructive to the information processing capabilities of Rolex Rings . The term is derived from the phrase “Malicious Software” and may also be called malicious code or commonly (but inaccurately) “a virus”.

#### 12.2 Anti-malware policy

In order to prevent the infection of Rolex Rings computers and networks and avoid the potentially dire consequences of such infection, there are several key controls that will be adopted as policy.

The key concept adopted in this policy is “defence in depth” and no single control should be relied upon to provide adequate protection. This is therefore not a choice between controls but a list of necessary controls, all of which should be implemented where possible to guard against the threats outlined in the previous section.

### 12.2.1 Firewall

A firewall will be enabled into the individual system is connected to the internet.

And all individual has responsibility not to disable the firewall.

### 12.2.2 Anti-virus

All individual has responsibility to keep antivirus up to date. IT Team will do continuous monitoring of the same.

Anti-virus programs generate audit logs of their actions.

Quarterly reviews of all anti-virus software must be completed to verify that they:

- Detect all known and new types of malicious software
- Remove all known and new types of malicious software
- Protect against all known and new types of malicious software

### 12.2.3 Spam filtering

A system will be installed to filter out unsolicited and potentially harmful emails (spam). Types of attachments known to often contain malware must be blocked or removed before delivery to the user.

### 12.2.4 Software installation and scanning

The IT Team will regularly monitor the environment to see if there are unapproved software installed in user systems. Users shall not attempt to install any software without IT and HOD approval.

### 12.2.5 Vulnerability management

Vulnerability scanning must be carried out twice a year for applications and quarterly for infrastructure, particularly on business-critical application.

For new vulnerabilities identified by Rolex Rings employees, the employee will report the same to IT team on [infosec@RolexRingsLtd.com](mailto:infosec@RolexRingsLtd.com)

### 12.2.6 User awareness training

Users must be made aware when starting with Rolex Rings of the information security policy and be trained in ways to avoid falling victim to attacks such as phishing.

This awareness training must be repeated on a regular basis to users who access the Rolex Rings business information. It also gets covered in the ISMS awareness training conducted at regular intervals.

### 12.2.7 Threat monitoring and alerts

Information about emerging threats will be obtained from appropriate sources and users alerted proactively of potential attacks, giving as much detail as possible to maximize the chance of recognition.

Malicious activity detection tool i.e., Securonix (SIEM), Seqrite (EPS), Deep Security (Trend Micro), Firewall is deployed to monitor the malicious activity or policy violations. Any detected activity or violation will be reported either to IT Team or collected centrally.

#### 12.2.8 Technical reviews

Regular reviews will be carried out of business-critical services to identify any malware that has been installed since the last review. This will include the taking of a snapshot of the configuration for later comparison purposes.

#### 12.2.9 Malware incident management

If malware is detected on a business critical services an information security incident will be raised. This will be managed in accordance with the procedures set out in the Information Security Incident Response Procedure.

### 13 Backup Policy

Regular backups of essential business information must be taken to ensure that Rolex Rings can recover from a disaster, media failure or other form of error.

The following criteria must be defined and agreed:

- Scope, schedule and location of backups
- Physical and logical protection measures
- Backup methods and data formats
- Retention periods for backups
- How the integrity of backups will be verified
- Restoration and testing procedures, including restoration timescales during a disruptive event
- Use of encryption wherever applicable
- Frequency and method of reviews of backup and recovery procedures

Full documentation of the backup and recovery procedure associated with each backup must be created and stored. Failed backups shall be completed manually.

Backup media shall be monitored by numbering and its use on a sequential basis

Regular restores of information from back up media must be performed to verify the reliability, accuracy and integrity of the back-up media and the restore process. Restoration shall be formally approved. A Backup Restoration Log shall be maintained to include, but not limited to, the following details:

- Date for data restoration;
- Personnel requesting the data restoration;
- Personnel approving the data restoration
- Personnel responsible for the restoration;
- Reason for data restoration; and
- Status – successful/unsuccessful

The restored contents shall be verified against the source system for an exact match. This shall be verified by IT support Team.

System documentation must be protected from unauthorized access (this does not include generic manuals that have been supplied with software). Effective version control must be applied to all documentation and its storage.

Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

Configuration files for all systems including but not limited to Servers, Network Storage, Routers, Switches, Firewalls, Wireless Access Controllers shall be backed up on a periodic basis with restricted access.

### 13.1 Backup logging and audit trail

Backup logs shall be recorded for all the backups taken and shall be reviewed on a daily basis by the IT Staff. The daily review shall include, at a minimum, the following details:

- The application / server for which the backup has been taken;
- The label of the media on which the backup had been taken;
- The status of the Backup – Successful/ Unsuccessful/ Incomplete; and
- Monitor schedule backup as per defined policy, take required action in case of backup failure and inform to respective server \ application owner.
- Backup failures shall be treated as incidents and shall be handled as per the Incident Management Policy.

### 13.2 Backup Storage

- Backup media shall be physically protected commensurate with the classification level.
- For critical backup, wherever possible, there shall be more than one copy of the data

| Asset Name                      | Frequency                    | Schedule | Type | Media                      | Retention Period | Mode   |
|---------------------------------|------------------------------|----------|------|----------------------------|------------------|--------|
| Switches (All Managed switches) | Monthly (1st of every month) | -        | Full | One Drive (Config. Backup) | 1 Month          | Manual |

## 14 Logging and monitoring policy

### 14.1 Audit logging

The processing of classified information will have the available audit logging facilities activated to allow the recording and monitoring of activities in the following areas based on system criticality:

- User ID of the person, performing activity
- Date and time for logon and logoff

Policy Adopted on May, 25, 2023

- Record of successful and failed system access attempt
- Device identity
- Changes to the system configuration
- Activities performed by super users
- Network addresses
- Activation & deactivation of key systems, such as antivirus server

The general principle adopted is that the higher the level of classification of the information held or processed, the greater the level of detail to which the audit logs will record data. Web access logs are excluded for now.

## 14.2 Monitoring system use

The contents of audit logs will be reviewed on a regular basis according to the:

- Business criticality of the application
- Classification of the information assets involved
- Frequency with which systems have been attacked or compromised previously
- Level of exposure to external networks

It is impossible to manually review all audited events within all audit logs, so it is important that the most critical systems are addressed first and that log events are filtered as much as possible.

The following events will be investigated as a matter of urgency:

- Unauthorized removable device attachment
- Changes to systems security settings and controls
- Alerts from intrusion prevention systems (Fortinet)
- Unusual use of privileged accounts e.g. administrator

Investigation will be carried out according to the procedures set out in document Information Security Incident Response Procedure.

## 14.3 Protection of log information

Strict permissions will be used to ensure that the contents of log files cannot be altered after they have been written. Where possible, key events from log files will be copied to a central point and archived. Backups of log files will be taken on a daily basis in real time via Securonix cloud. Logs will be retained and saved for 365 days in Securonix cloud.

## 14.4 Administrator and operator logs

Logs will be taken of all administrator and operator activities where feasible so that it is possible to identify the actions that were carried out under such user accounts. Whilst this may not be necessary for every system within Rolex Rings, those holding classified information or involving a financial element will be monitored more closely.

## 14.5 Fault logging

Error logging will be enabled on all systems and applications dealing with classified information and all reported faults will be investigated to ensure that security controls have not been compromised. Faults will be logged and investigated according to Rolex Rings' standard incident management process.

## 14.6 Clock synchronization

All systems will synchronize their date and time with NTP server and be maintained at UTC time. This is important so that events on different systems can be correctly compared during incident investigation without having to consider differences in system times.

## 15 Software Policy

This policy sets out how software will be acquired, registered, installed and developed within Rolex Rings . An up-to-date inventory will be kept and maintained of installed software within Rolex Rings .

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Rolex Rings systems.

The following policies and procedures are relevant to this document:

- Acceptable Use Policy
- Change Management Process
- Mobile Device Policy

### 15.1 Use of software on-premises

#### 15.1.1 Purchasing software

All computer software to be used within Rolex Rings must be purchased through Rolex Rings IT team. This is necessary to ensure that:

- Licensing requirements are addressed
- Use of the software can be supported by the IT Team
- Best value for money is obtained in procurement

Under no circumstances will software be purchased using local departmental budgets.

#### 15.1.2 Software Registration

All software in use within Rolex Rings must be correctly licensed where feasible. Where this is open source software, Rolex Rings will ensure VA of the same. All open source software should be listed as exceptions.

All installed software programs will be registered in the name of Rolex Rings , not the individual. Purchased software is a corporate asset and licenses will frequently be reused as the shape of the organization changes.

Under no circumstances must corporate software be copied (other than for backups) or installed for use on non-corporate machines, such as at home.

Rolex Rings IT will maintain a register of all licensed software within the organization and licensed copies of media.

Asset management software will be used to keep track of all installed instances of software titles and regular audits will be carried out.

#### 15.1.3 Software Installation

Software will be installed by Rolex Rings IT Team or appropriate technical team or supplier upon request.

Policy Adopted on May, 25, 2023

Software will not be installed prior to approval of IT head

The user must not install any software by themselves

#### 15.1.4 Removal of software

If a software program is no longer required, Rolex Rings IT Team must be informed. The software will then be removed from the device in question and where possible the license will be re-used elsewhere within Rolex Rings .

Users must not remove licensed software from their devices without informing Rolex Rings IT Team as this potentially represents a waste of a corporate asset.

#### 15.1.5 In-house software development

Rolex Rings does not develop any software or application on premises, except for the customized changes requested by users. And these changes leads to minor developments. The minor change requests are only for SAP & BI reporting tool. So, the development team follows the approved change management procedure

Refer change management procedure for more details.

### 16 Technical vulnerability management policy

#### 16.1 What is a technical vulnerability?

A vulnerability is commonly defined as “an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

Rolex Rings ’s policy with respect to technical vulnerabilities is to be aware of them and to close them immediately where possible, either directly or via other means.

#### 16.2 Sources of information

The first step in managing technical vulnerabilities is to become aware of them. Since we are talking about technical vulnerabilities these will of course depend upon the technology employed within Rolex Rings . It is necessary then to gain a full appreciation of the technology components that make up Rolex Rings ’ s infrastructure and their versions (since most technical vulnerabilities are very version-specific).

This should include:

- Databases e.g. Sybase, MySQL, MSSQL
- Web servers e.g. IIS, Tomcat Apache,
- Desktop software e.g. Windows, Ubuntu. Cent OS, Suse and office productivity tools
- Web technologies e.g. Django, WordPress
- Application software e.g. Zoho Assist, Team Viewer etc
- Email Services e.g. O365 (Office Suite)

A process must therefore be put in place to ensure that all relevant information about updates is being received and reviewed by competent staff members. This will usually give guidance about the level of urgency associated with each update.

Where configuration changes are recommended to close off vulnerabilities, these must be actioned through Rolex Rings change management process so that appropriate controls are in place for testing, risks assessment and back out.

### 16.3 Patches and updates

Procedures will be put in place to obtain copies of the software updates electronically when they are issued by the vendor. The scheduling of the installation of updates will depend upon several factors including:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages to users)
- Co-ordination of the updating of related components of the infrastructure
- Dependencies between updates

The patch management will be followed through change management process for critical devices (example Server, Firewall, Switches etc). Endpoints are excluded. (see Rolex Rings Change Management Process).

### 16.4 Vulnerability assessment

Rolex Rings will conduct a vulnerability assessment at least twice in a year for applications and every quarter for network and server. An authorized third party vendor conducts the VAPT.

The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

### 16.5 Awareness training

As a result of a vulnerability assessment, it may be necessary to increase efforts in security awareness training for employees and contract staff. This training should explain the nature of vulnerabilities and what can be done to reduce them.

As part of awareness training, a phishing simulation exercise will be conducted on a regular basis. This will involve the sending of emails to employees that are intended to be similar to typical phishing messages, but which simply report to a central point within Rolex Rings if the requested action is performed by the employee, for example clicking on a link or opening an attachment. These exercises will help to assess the effectiveness of the awareness training delivered in recognizing and avoiding malware disguised in emails.

## 17 Change Management Policy

Rolex Rings policy with respect to the management of changes is as follows:

- Service components and other items that are under the control of change management are all critical software, hardware, supporting utilities and documentation that constitute a live service to Rolex Rings users or that may impact the data centre operations
- Endpoints will be an exception to change management.
- A single focal point will be established and maintained, through which all changes will be managed in order to minimize the likelihood of conflicting changes being carried out.
- In order to decide which, route a change should take through the process, change requests will be categorized based on their estimated resource requirement, urgency and risk
- The following categories of change will be used:
  - A standard/new system change is a small, low risk change that can be implemented in a short-governed time frame.
  - A normal change is one which has not been pre-classified as a standard change and is not an emergency.

Policy Adopted on May, 25, 2023

- o Emergency changes are changes which are urgently required in order to resolve a critical incident or problem.
- Changes must be assessed from the dual perspective of technical and business risk.
- Application head can approve the change requests for applications
- For IT Infrastructure changes, IT infra manager and IT head approval is required

## 18 Email Security policy

### 18.1 Sending and receiving electronic messages

Rolex Rings provided electronic messaging facilities must always be used when communicating with others on official business. You must not use a personal account for this purpose.

Rolex Rings maintains its legal right to monitor and audit the use of electronic messaging by authorized users to assess compliance to this policy.

Deletion of a message from an individual account does not necessarily mean that it has been permanently removed from Rolex Rings ' s IT systems and such messages may still, be subject to audit and review.

Particular care must be taken when addressing messages that include classified information to prevent accidental transmission to unauthorized recipients.

Users must avoid sending unnecessary messages to distribution lists, particularly those with wide circulation such as the "global list" of all employees. Where required, such messages should be sent via certain approved email ids.

Nothing must be sent externally which might affect Rolex Rings ' s reputation or affect its relationships with suppliers, customers or other stakeholders.

In particular, users must not send messages containing material, which is defamatory, obscene which a recipient might otherwise reasonably consider inappropriate. If you are not sure whether your intended message falls into this category, please consult your HOD/IT Team before sending.

Official organization Email facilities must not be used:

- For the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organizations
- To send material that infringes the copyright or intellectual property rights of another person or organization
- For activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- To distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- To send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- To convey abusive, threatening or bullying messages to others
- To transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs
- For the transmission of defamatory material or false claims of a deceptive nature
- For activities that violate the privacy of other users
- To send anonymous messages - i.e. without clear identification of the sender
- For any other activities which bring, or may bring, Rolex Rings into disrepute

If you receive unsolicited junk messages or spam, it is advised that you delete them without reading them. Do not reply to the message as this can confirm the existence of a valid address to the sender, resulting in further unwanted communications. For more guidance, contact Rolex Rings IT team at [itsupport@RolexRings.com](mailto:itsupport@RolexRings.com).

## 18.2 Monitoring of Email facilities

Email usage within Rolex Rings system is monitored and recorded centrally in order to:

- Plan and manage its resource capacity effectively
- Assess compliance with policies and procedures
- Ensure that standards are maintained
- Prevent and detect crime
- Investigate unauthorized use

Monitoring will be undertaken by staff specifically authorized for that purpose. Consistent monitoring procedures will be applied to all users and may include checking the contents of messages.

If a manager suspects that the electronic messaging facilities are being abused by a user, they must contact the IT Support Team. All such reports will be investigated by competent persons from IT team and where appropriate, evidence provided.

Users must not access another user's electronic messaging account unless they have obtained permission from the HOD and the HR Head. In such cases this must be for legitimate business reasons and only messages which may reasonably be judged to be relevant to the question in hand should be opened.

## 18.3 Use of email

In addition to the policy statements in other sections of this document, the following applies specifically to the use of email.

All e-mails sent from organization addresses to recipients outside of Rolex Rings will automatically carry the following disclaimer:

"DISCLAIMER

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this email and then delete it from your system. The entity is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt."

Mailbox will be set up with a limitation on its size (50 GB for E1 licence and business basic/100 GB for E3 licence). This is in order to prevent the available storage capacity from being exceeded and to ensure the cost-effective use of email.

You must manage your email account(s) to remain within the mailbox size limit, making use of the archiving facility included in most email clients where possible. If your mailbox has filled up, contact the IT Team for advice in the first instance.

Rolex Rings provides anti-virus software which runs on every computer that has access to the network and is intended to detect any viruses before they have been installed.

In addition, you must not:

- Transmit by email any file attachments which you know to be infected with a virus
- Download data or programs of any nature from unknown sources
- Disable or reconfigure the installed anti-virus system operating on a computer used to access email facilities
- Forward virus warnings other than to the IT Security (infosec@Rolex Rings Ltd.com)

If a computer virus is deliberately or accidentally sent to another organization, Rolex Rings could be held liable if the transmission could be considered negligent.

## 19 System Acquisition, Development, and Maintenance Policy

### 19.1 Security requirements of information systems

The security requirements shall be identified and agreed upon prior to the development of an information system. Security requirements shall be justified and agreed with Business Heads.

All security requirements, including the need for fallback arrangements, shall be identified at the requirement phase of a project, then justified, agreed upon and documented as part of the application's overall business case. Statements of business requirements for new applications, or enhancements to existing applications; shall specify the requirements for security controls.

Security requirements and/ or security specifications, either explicitly or by reference, shall be included in master service agreement. If Rolex Rings acquires any software from third-party vendor, its functional testing shall be performed before deploying it in the production environment. Supplier shall ensure that adequate information security requirements are addressed in their product. Vendor shall be required to submit the results of independent testing performed such as code review, Vulnerability Assessment and Penetration Testing (VAPT), to demonstrate that their product is secure. This may be done / arranged by Rolex Rings depending upon the agreement with the Vendor, and also be covered as a part of periodic VAPT Assessments alongside other applications / systems.

Any web application which is hosted on public network shall be protected by using adequate encryption technology for protection against external threats. Also,

adequate security controls shall be put in place for any data which is shared with third party/ customer/ vendor over public network.

IT Team shall ensure that security controls are implemented to prevent incomplete transmission, miss-routing, repudiation of transaction, unauthorized message duplication and replay. Controls to consider include:

- Validating and verifying user credentials
- SSL based encryption of data in transit
- Secure communication protocols
- Storing online transaction details on servers within the appropriate network security zone

## 19.2 Security in development and support processes

In order for applications to be designed and implemented with proper security requirements, secure coding practices and a focus on security risks shall be integrated into day-to-day operations and the development processes.

### 19.2.1 Secure development

A secure development environment shall be maintained and include separate development environment from production environment. Deviation to this shall be formally approved. Development, testing and production environments shall be segregated to reduce the risk of unauthorized access or unauthorized change to the IT system. It shall be ensured that all systems and software used in the development environment are regularly patched with the latest security patches/ upgrades. Also, all systems shall have an Antivirus software which shall be regularly updated with the latest signatures. Administrative access to end systems shall be restricted and internet access on these systems will be limited to certain approved websites.

The implementation of changes within the entire development life cycle shall be controlled by the use of formal change control procedures. Introduction of new applications, major changes to existing applications and modifications to software packages shall follow a formal process of documentation, specification, testing, approvals, and managed implementation (Refer Change Management Policy).

### 19.2.2 Acceptance Testing

The Development team shall organize the developed/ customized software to be tested by end user(s) for acceptance. The Development team and IT team shall be involved in planning test cases for User Acceptance Testing (UAT). A separate test environment shall be created on which any changes/ patches will be tested before

deploying the same in production environment. The IT team shall be responsible for carrying out the testing and subsequent deployment in production. For any functionality changes, business team shall also be responsible for performing UAT.

UAT shall cover but, not limited, the below:

- Adequacy of the implementation for the requirements specified
- Any changes in the mode of operations after the requirement analysis phase
- Any changes in the statutory/regulatory requirements
- Adequacy of the security controls

### 19.2.3 Test data

The below mentioned guidelines shall be followed to ensure protection of data used for testing:

- Test data shall be selected carefully, protected and controlled. The use of production data that contains Personally Identifiable Information (PII), confidential or sensitive customer information may be avoided for testing.
- If there is a requirement to copy production data in the test environment, appropriate documented authorization from the application head shall be obtained with justification

## 20 Information security policy for supplier relationships

### 20.1 General provisions

In general, information security requirements will vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

However, the following will generally apply.

- The information security requirements and controls must be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract
- Separate Non-Disclosure Agreements must be used where a more specific level of control over confidentiality is required
- Appropriate due diligence must be exercised in the selection and approval of new suppliers before contracts are agreed
- Remote access by suppliers must be via approved methods that comply with our information security policies
- Access to Rolex Rings information must be limited where possible according to clear business needs
- Basic information security principles such as least privilege, separation of duties and defence in depth must be applied
- Where applicable, sub-contract clause and controls will be defined in the agreement and implemented
- Incident management and contingency arrangements must be put in place based on the results of a risk assessment

### 20.2 Addressing security within supplier agreements

For vendor selection in Rolex Rings , a request is sent to the purchase department with the details of requirements of the services requirement. After evaluation, the vendor is finalized and on-boarded

Policy Adopted on May, 25, 2023

into Rolex Rings IT. A list of checkpoints that will be applicable to all vendors generally is maintained.

The security requirements will be mentioned in the contract. All vendors shall sign an NDA.

### 20.3 Evaluation of existing suppliers

Rolex Rings follows continuous evaluation of suppliers to check performance deliveries and meetings are held with the vendor persons when required.

### 20.4 Managing changes to supplier services

#### 20.4.1 Changes within contract

Changes to services provided by suppliers will be subject to the Rolex Rings change management process. This process includes the requirement to assess any information security implications of changes in contract so that the effectiveness of controls is maintained.

#### 20.4.2 Contractual Disputes and end of contracts

In the event of a contractual dispute or end of contract, there will be a joint decision made by the IT Head, CISO and the Legal department. Purchase department will be involved if required. At all times the degree of risk to the business, in both technology and finance must be managed and if possible minimized.

#### 20.4.3 Exception

This policy does not apply to the current vendors and their functioning will stay as it is. This will be applicable on new agreements and contracts i.e. after January 9, 2023. It is to be noted that it will also be applicable to renewed agreements.

## 21 Incident Management Policy

### 21.1 Policy statement

All security breaches or attempts to breach or incident and all discovered security weaknesses in information systems and processing facilities shall be reported. The information security incident management process shall ensure that all reported security breaches or weaknesses are responded to promptly and appropriate actions taken to prevent re-occurrence.

**Definition:** Any event which causes, or may cause, an unplanned interruption to, or reduction in the quality of that service is termed as an 'incident'. The term 'incident' can be defined as any irregular or adverse event, which occurs on any part of Rolex Rings IT systems

### 21.2 Policy Details

#### 21.2.1 Incident Management

- Incident is an unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a Configuration Item that has not yet impacted service is also an Incident.
- Incidents can be reported by users or discovered within the IT environment by automation or support personnel
- Investigation may or may not involve understanding the cause of an incident. The primary objective is to recover service.

- Investigation (root cause analysis) into underlying cause and identification of critical and high priority incidents will be done, excluding end-user devices and end user applications
- Categorization of the incidents is done based on the severity of the incidents;
- Corrective actions are defined based on the category of the incidents;
- Planning and implementation of corrective action to prevent recurrence is carried out, if necessary;
- All Incidents shall be prioritized based on the severity of the Incident.(Refer Annexure 22 A)
- Escalation matrix is defined based on the category of the incidents; (Refer Annexure 22 B)
- All emergency actions taken are documented in detail, escalated as per escalation matrix (Annexure 22 B) and reviewed in an orderly manner. The action plan shall include:
  - Particulars about the business unit or department etc.;
  - Facts and explanation/reasons for the incident;
  - Description of resolution taken;
  - Estimated cost of implementing the corrective action (if any); and
  - Estimated time-frame, start date and end date.

#### 21.2.2 Reporting information security events and weakness

- A formal information security incident management process including incident reporting, incident response, escalation and incident resolution shall be established
- Employees and third-party staff shall be made aware of their responsibilities and process for reporting the security incidents that they observe or suspect
- Responsibilities shall include and explicitly state that they should not be involved in committing security breaches or attempting to prove the suspected security incidents. This should also be part of the Information Security Awareness Program
- In addition, the users shall not test the existence of vulnerability in any information system and/ or facility

#### 21.2.3 Collection of evidences

- As per the legal requirements the evidences shall be collected during incident analysis, retained and presented for relevant authorities for the major/ critical incidents The evidence shall be collected in a manner that does not destroy its evidentiary value
- While collecting the evidence, the following should be considered:
  - o Applicability of evidence: Whether the evidence can be used in a court of law; and
  - o weight of evidence: the quality and completeness of the evidence

#### 21.2.4 Annexure

| Severity | Level | Description |
|----------|-------|-------------|
|----------|-------|-------------|

|          |   |                                                                                                                                                                                                                                             |
|----------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | 4 | Direct threat or damage to image, reputation or credibility of Rolex Rings . Multiple business functional units getting severely impacted. Location of business critically affected. Business continuity measures would have to be invoked. |
| High     | 3 | Severe outage affecting single business functional units, key services or location.                                                                                                                                                         |
| Moderate | 2 | Moderate degradation to business functional units, locations, IT assets. Moderate to high impact to non-critical business units within Rolex Rings .                                                                                        |
| Low      | 1 | Small issue with localized scope. Affecting few resources. Issue can be tolerated for a particular period of time                                                                                                                           |

Annexure 22 A: Incident Management Severity Matrix

Annexure 22 B: Incident Management Escalation Matrix

| Level   | Contact Person                                |
|---------|-----------------------------------------------|
| Level 1 | IT Application or Infrastructure support team |
| Level 2 | IT Application or Infrastructure Head         |
| Level 3 | Head of IT                                    |

## 22 Availability management policy

### 22.1 Availability monitoring and reporting

A network monitoring tool will be used to ensure that all critical business assets are available.

Rolex Rings will also monitor the availability of key components that support the services provided so that data is available for analysis when investigating the causes of service outages.

Availability statistics will be published as part of the management reporting cycle and will refer back to the targets agreed. Where a target has not been met, some indication of the reason and actions that are to be taken will be given.

### 22.2 Non-availability

#### 22.2.1 Planned

Where it is necessary for Rolex Rings to withdraw a service as part of planned activities, the length of notice will be agreed. This may be for scheduled maintenance or for the implementation of changes that have been approved as part of the change management process.

Planned unavailability will be communicated to all users via the intranet. Warning emails will also be sent out in the run up to the scheduled outage from a generic support ID.

### 22.2.2 Unplanned

In the event of a service needing to be withdrawn as a result of an incident, Rolex Rings IT Team will make all reasonable endeavors to keep users informed of the status and likely restoration of the service.

The causes of unplanned non-availability will be investigated, and a report produced stating what will be done to prevent a re-occurrence. Any improvements identified will be managed through the change management process.

### 22.3 Availability plan testing

In conjunction with the business continuity testing schedule, availability plans will be tested on a regular basis and on major changes to services to ensure they remain effective. Reports will be produced from these activities and improvements identified.

### 22.4 Impact of changes

As part of the change management process, all change requests will be assessed for implications to availability plans and these plans will be amended appropriately as part of the change. This will ensure that availability plans do not become out of date as the IT environment develops.

## 23 Records retention and protection policy

Record retention will be done as per the information asset inventory.

### 23.1 General principles

There are several key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must always remain retrievable in line with business requirements

### 23.2 Record types and guidelines

Information about records held by Rolex Rings , including their security classifications and owners can be found in Information Asset Inventory.

### 23.3 Use of cryptography

Where appropriate to the classification of information and the storage medium, Cryptographic techniques may be used to ensure the confidentiality and integrity of records.

Care must be taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with Rolex Rings ' s policy on cryptography (see Cryptographic Policy).

### 23.4 Record retrieval

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time.

Policy Adopted on May, 25, 2023

### 23.5 Record destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used.

The procedure allows for the correct recording of the details of disposal which must be retained as evidence.

### 23.6 Record review

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting business requirements]

The information asset inventory must be reviewed once in a year

The results of these reviews must be recorded.

## 24 Privacy and personal data protection policy

### 24.1 Privacy by design

Rolex Rings has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues.

Rolex Rings conducts regular security assessments to safeguard its data assets therefore protecting the PII of the stakeholders.

### 24.2 Breach notification

It is Rolex Rings' policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. Where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority (CERT-IN) will be informed within 6 hours. This will be managed in accordance with Rolex Rings' Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

## 25 Internal Audit Policy

The Objective is to conduct internal audits at planned intervals to verify if the the Information security management system are implemented and maintained effectively.

### Policy Description:

- There shall be Internal Audits held at planned intervals to determine whether the Information Technology Security Policy being delivered fulfil the requirements.
- Internal Audit shall assess if Information Technology Security Policy being delivered are effectively implemented and maintained.

Policy Adopted on May, 25, 2023

- The authorities and responsibilities for planning an audit program, conducting audits, reporting results and maintaining audit records shall be documented.
- Audit scope, frequency and methods shall be documented. Audit Program shall be planned considering the status, importance of processes/areas to be audited and results of previous audits.
- Internal Audit shall be conducted at least once in a year based on audit criteria.
- For ensuring objectivity and impartiality of the audit, auditors shall not audit their own work
- Records of audits and their results shall be maintained in secured and protected environment. Non-conformities shall be documented, communicated, prioritized with responsibility allocated for actions.
- Auditee/respective management responsible for the area being audited shall take necessary timely corrections, corrective actions, preventive actions as applicable shall be documented, to eliminate non-conformities and their causes respectively.
- Actions will be verified by the auditors for closing the non conformance.
- Audit reports shall be analyzed and shared during management review meetings. The opportunities for improvement to the Information Technology Security Policy being delivered will be identified based on the analysis.
- Closure times shall be 1 week, 2 week and 3 weeks respectively for Major Non-Conformity, Minor Non-Conformity and Observations respectively.

## 26 Network security policy

### 26.1 Network security design

This policy does not attempt to specify how individual networks should be designed and built but provides guidance for the standard building blocks that should be used.

#### 26.1.1 Requirements

A network design must be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities
- The level of trust between the different components or organizations that will be connected
- The hours of availability and degree of resilience required from the network
- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will be used for access
- Requirements must be documented and agreed before design work starts.

#### 26.1.2 Defence in depth

A “Defence in Depth” approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network.

### 26.1.3 Network segregation

Where appropriate, a network networks will be segregated from each other based on either trust levels or organizational boundaries (or both).

For a large network this may be achieved using separate domains, particularly where separate organizations’ networks are being linked. An appropriate level of trust must be configured at the domain level and domain perimeters must be secured using a firewall where appropriate.

### 26.1.4 Perimeter security

At all perimeters between the internal network and an external network (such as the Internet) effective measures must be put in place to ensure that only authorized network traffic is permitted. This will usually consist of at least one Stateful Inspection firewall and for major links with the Internet an Application (or Application Gateway) firewall must be used. For connections such as internet leased line at smaller locations a Packet Filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network (such as web servers) must be located in a De-Militarised Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

### 26.1.5 Public networks

Where information is to be transferred over a public network such as the Internet, strong encryption via TLS must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

### 26.1.6 Wireless networks

Wireless networks must be secured using WPA2 encryption. WEP and WPA must not be used.

WPA2 is used as the encryption method

A guest wireless network may be provided for visitors. This must be logically separate from all internal networks (including internal wireless networks).

Wireless access points must be configured to not allow connection using WPS (WiFi Protected Setup) via physical access to the access point itself.

Wireless access point admin logon passwords must always be changed from the default.

### 26.1.7 Physical security

Remote network equipment will be housed in secure cabinets which will always be locked. Only support staff will have access to the key to each cabinet.

Backbone and centralized network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to which only authorized support staff will have access (except for local facilities staff for reasons of health and safety).

Wireless access points located in public areas must be hidden from view where possible and must be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing must be installed where an access point is located in an unprotected public area e.g. a car park.

#### 26.1.8 Remote access

Where there is a requirement for remote access to the internal network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using IPSec
- Two factor authentication at the client where appropriate
- Secure authentication using a LDAP (SAML 2.0) server
- Firewall will be used to restrict access to remote clients that do not meet minimum requirements e.g. virus control

Remote access must be granted on an “as required” basis rather than for all users by default. Formal authorization must be obtained from IT head and department HOD for the same.

#### 26.1.9 Network intrusion detection

A Network-based Intrusion Detection and Prevention System (NIDS/NIPS) must be installed at the network perimeter and at all key points within the network e.g. on critical servers. For networks with high security requirements an Intrusion Prevention System (IPS) may be preferred.

#### 26.1.10 Network security standards

The following standards will be adopted with respect to network configuration and security.

#### 26.1.11 Network hardware

Network routing will be based on Fortinet SD-WAN. Cisco switches will be used as standard for connectivity. Switch ports, including diagnostic ports, will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security weaknesses.

Cat 6 UTP will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

#### 26.1.12 IP addressing

IPv4 will be used on internal networks. However new network devices purchased must support IPv6 in preparation for the future.

The internal IP address range used will be 192.168.0.0 – 192.168.254.254. the assignment and use of subnets must be monitored carefully. For VPN, the IP address range will be 10.10.16.0/24, and 10.10.24.0/24

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP or statically. Internal DNS servers will be used.

#### 26.1.13 Network protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server will be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

## 26.2 Network security management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure networking environment to protect Rolex Rings' s information in systems and applications. This must be achieved via controls in the following areas.

### 26.2.1 Roles and responsibilities

Roles and responsibilities for the management and control of networks must be clearly defined. In order to provide effective segregation of duties, the operation of networks is managed separately from the operation of the rest of the infrastructure such as servers and applications.

This segregation of duties is detailed in the following table.

| Manger Role     | Team               | Areas of responsibilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Manager | Network Security   | <p>Manage Network architecture including passive and active components.</p> <p>Install, Build and Managing Network Infrastructure, Evaluate modern technologies.</p> <p>Operate and support for Monitoring of network, expansion and new projects.</p> <p>Network security monitoring and confirm compliance.</p> <p>Enhancement of security and continue validate its covering.</p> <p>Network monitoring tools, VAPT, Optimization projects.</p> <p>Coordinate with ISP in case of problems, design redundancy and ensure stable network.</p> <p>Arrange ISP with its prerequisites, Configuration of Firewall, Switches, Router, WiFi devices.</p> <p>Managing and Coordinating with Partners and OEM for support.</p> <p>Manage and resolve incident in timely manner and ensure Business Operations carried out smoothly with OLA/SLA committed and adhered too.</p> <p>Manage and create Documents and versions for IT Audits. Participate in IT Audits and ensure remediation in timely manner.</p> <p>Manage IT Security and Monitor Security Events and Alerts.</p> <p>Independently work as an in-charge of NOC and ensure demanded up-time.</p> |
| FMS Team        | Network Operations | <p>Network availability monitoring.</p> <p>Coordination with ISP and Vendors.</p> <p>Second line incident management.</p> <p>Network Troubleshooting.</p> <p>Configuration backups</p> <p>Patching and updates.</p> <p>Setup and management of remote access users.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 4: Roles and responsibilities

### 26.2.2 Logging and monitoring

Logging levels on network devices must be configured in accordance with organization policy (see Logging and Monitoring Policy) and logs monitored on a regular basis.

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Prevention System must be configured to alert the Network Operations team of this activity. Firewall logs will be stored for 90 days.

Network monitoring for availability may be achieved using an appropriate SNMP based network management tool (EMCO) and recovery actions automated where possible.

Alerts from the SIEM and Firewall system must be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a required subset of systems on the network.

### 26.2.3 Network changes

All changes to network devices will be subject to the change management process and appropriate risk assessment, planning and back-out methods put in place. A current and accurate picture of the network is always maintained.

Change or Service tickets will be raised as appropriate.

### 26.2.4 Network security incidents

Network events which are deemed to be security incidents must be recorded and managed according to the Information Security Incident Response Procedure.

## 27 Cloud Security Policy

It is Rolex Ring policy in the area of cloud computing that:

Data belonging to Rolex Ring will only be stored within cloud services with the prior permission of the Chief Information Officer.

Appropriate risk assessment must be carried out regarding proposed or continued use of cloud services, including a full understanding of the information security controls implemented by the CSP.

Due diligence must be conducted prior to sign-up to a cloud service provider to ensure that appropriate controls will be in place to protect data. Preference will be given to suppliers who are certified to the ISO/IEC 27001 international standard and who comply to the principles of the ISO/IEC 27017 and ISO/IEC 27018 codes of practice for cloud services.

Service level agreements and contracts with cloud service providers must be reviewed, understood and accepted before sign-up to the service.

Contracts involving personal data must be checked to ensure that they comply with applicable data protection legislation. If not, a separate data processing agreement may be required.

Roles and responsibilities for activities such as backups, patching, log management, malware protection and incident management must be agreed and documented prior to the commencement of the cloud service.

Procedures must be established to ensure that activities that are irreversible in the cloud environment (e.g. deletion of virtual servers, terminating a cloud service or restoration from backups) are subject to appropriate controls to avoid error. Supervision by a second, suitably qualified person must be a stated part of such procedures.

The location of the data stored with the CSP must be understood e.g. UK, EU, USA and the applicable legal basis established, such as the country whose law applies to the contract.

Where available, multi factor authentication must be used to access all cloud services.

Sufficient audit logging must be available to allow Rolex Ring to understand the ways in which its data is being accessed and to identify whether any unauthorized access has occurred.

Confidential data stored in cloud services must be encrypted at rest and in transit using acceptable technologies and techniques. Where possible encryption keys will be held by Rolex Ring rather than the supplier.

Rolex Ring policies for the creation and management of user accounts will apply to cloud services.

Backups must be taken of all data stored in the cloud. This may be performed either directly by Rolex Ring or under contract by the cloud service provider.

All Rolex Ring data must be removed from cloud services in the event of a contract coming to an end for whatever reason. Data must not be stored in the cloud for longer than is necessary to deliver business processes.