# 4. END USER RESPONSIBILITIES


Institutions around the world are facing an increasing number of challenges to keep organizational assets secure and safe from intrusion. On one hand, cyber attackers are becoming more sophisticated and there are more and more ways to get access to an organization's network to steal data or trigger malicious attacks that lead to the disruption of operations. On the other hand, since almost everyone has access to a smart phone, laptops and portable storage devices, and all of these devices have the potential to connect with organizational networks, actions of an inadvertent insider may lead to leakage of confidential information or misuse of resources.

It is said that humans are the weakest link in the information security chain and 95% of the cyberattacks are caused by human error. Therefore, contribution of users at all levels is required to maintain a high level of information security and security should be an integral part of everybody's job profile and objectives.

### OBJECTIVE

To ensure that all users of an organization understand their responsibilities in relation to protecting information assets, computer systems and digital infrastructure owned by the organization.

# 4.1. End User Responsibilities in General

An end user is the person who uses computers systems, digital infrastructure, or Internet and email. End user responsibilities are summarized below. Specific roles and responsibilities of Information Security Officers (ISO), Associate Information Security Officers (AISO), and Chief Innovation Officers (CIO) are presented in Chapter 3.

## 4.1.1. Adherence to Regulatory Requirements and Polices

The functions of government organizations are subject to many regulatory requirements. Protection of information is required to protect the interests of the organization and its clients. The users are, therefore, required to ensure that they understand and adhere to applicable regulations. Further, users must comply with all policies and guidelines set by the organization in relation to information technology and security.


## 4.1.2. Ensure Secrecy of Information Assets

Information Security is a responsibility of all employees. All staff, temporary workers or contractors who are accessing the government information are required to respect the confidentiality and security of that information. Users are not authorized to copy or distribute confidential data, photographs, copyrighted software or any other information asset prohibited by the government organization under any circumstances.

### 4.1.3. Protection of Intellectual Property

Users must protect the intellectual property of the organization or such property under the custody of the organization. Downloading, redistributing and printing of such intellectual property is strictly prohibited.

John and Karen had an open marriage.

### 4.1.4. Ensure the Protection of Credentials

The safe-keeping of each user credential is the responsibility of the user to whom it is entrusted. Users must not disclose the credentials to anyone.

### 4.1.5. Unauthorized Entries

Users should not attempt to make unauthorized entries to system devices or networks or access information assets which they are not expressly authorized to access.

### 4.1.6. Install Unauthorized Software

Users are prohibited from introducing unauthorized copies of software to the organization's digital infrastructure. Users shall not install system utilities, third party software or security patches which are not supplied by the organization.

### 4.1.7. Personal Use of Systems

All users must refrain from using organization's resources for personal or private business purposes or for entertainment.

### 4.1.8. Plug in Unauthorized Devises

Users must not connect any hardware devises to organization's computers and networks without approval from the ISO. Such devices include mobile computing devices (tabs, laptops etc), mobile phones, digital cameras or removable media including floppy disks, Compact Disks, DVDs, Flash drives, mp3 players or similar devices.

### 4.1.9. Configuration of Devices and Networks

Users are strictly prohibited from configuring devices and software of the organization. Further, users must not post network or server configuration information about any government organization's information systems on public newsgroups or mailing lists.

### 4.1.10. Prevent Engaging in Malicious Actions

Users must not purposefully engage in activity that involves stealing from, harassing, threatening or abusing others, or actions that degrade the performance of networks (or devices) and Information Assets, or gather information through social engineering or perform cyber-attacks or any other activity that could lead to cyber incidents.

### 4.1.11. Reporting Incidents


All users are strictly advised to immediately report of any evidence or suspicion of any security violation to the Information Security Officer. Security violations would include but are not limited to (1) unauthorized access to a network, telecommunications or computer system, (2) the apparent presence of a virus on computers, (3) the apparent presence of any information resource prohibited by guidelines, (4) apparent tampering with any file for which the user established restrictive discretionary access controls, and (5) violation of these Guidelines or security policy by another user or contractor.

### 4.1.12. Facilitating Incident Investigations

Users are expected to assist and facilitate incident investigations by providing as much detail as possible about the incidents that they observe, as well as to preserve related evidence, and to make themselves available to offer assistance as the incident response progresses. Organization should grant anonymity in the event they are reporting a breach caused by another employee.

### 4.1.13. Reporting Vulnerabilities

Users must report all identified vulnerabilities to the RMC immediately. Vulnerabilities may exist on information assets, computer systems or any other digital infrastructure. The party identifying such vulnerability must not disclose them to unauthorized personnel.

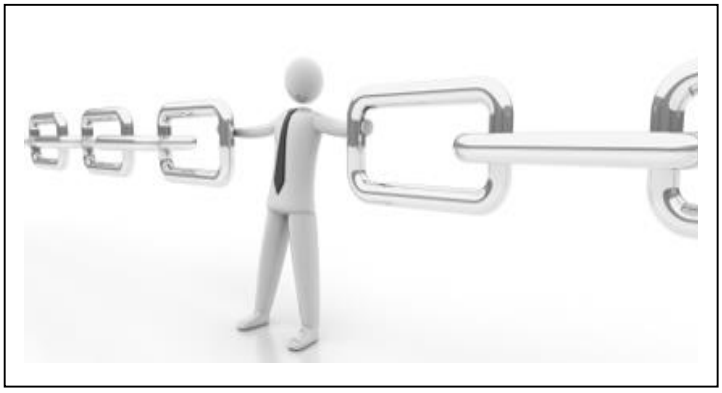
> Users must not exploit the vulnerabilities of the system or information assets.
>
> *Box 4A*

### 4.1.14. Pornographic Material

Introduction of pornographic material into any government organization's information system environment is strictly prohibited. The storage, processing, or transmission of pornographic material on the government organization's information systems, by the organization's employees, contractors, or associates, is strictly prohibited.

### 4.1.15. Rights-to-Audit

At any time and without prior notice, the organization reserves the right to examine E-mail, personal file directories, and other information stored on the government organization's computers.



## 4.2. Safe and Appropriate Use of E-mail

### 4.2.1. Use Official E-mails

Organization should use emails with “gov.lk” domain for official communication, and each employee should use official email for official communications (official emails are the email supplied by the government with the domain name of “gov.lk”). Employees must not use official emails for personnel communications.

***Policy Statement 11:***

***Organizations Should Use Official Emails for Official Communications***

*Applicable to all organizations*

Official email account is an official asset and the organization has the right to access, read emails or delete the account.

### 4.2.2. Email Scanning

All email attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any government organization’s computer system. Furthermore, users must not install any upgrades or patches or execute any programs received via E-mail.


Users must perform a virus scan on all material that is transmitted to other users via E-mail prior to sending it. Receipt of emails with suspicious content or attachments, and any other suspicious event should be report to Incident Response Team immediately.

### 4.2.3. Unauthorized Access and Modification

Users must not attempt to gain access to emails of other users or attempt to modify the content of emails sent by or directed to another person.

The user of an organization's e-mail system is a visible representative of the organization and therefore, users must use the system in a legal, professional and responsible manner to uphold the reputation of the organization.
*Box 4B*

### 4.2.4. Appropriate Content

Each user is responsible for all text, audio, video, or image content that they place or send over the official e-mail. Users must not use official emails in a manner that is harmful, disruptive or offensive for the recipients. Further, official emails should not be used to communicate obscene content, politically motivated content or any other inappropriate content.

### 4.2.5. Ensure Confidentiality

Government users must not use emails for sharing confidential (sensitive Information) without applying appropriate encryption techniques, as emails can be intercepted or accidentally be exposed. Clear text information in transit may be vulnerable to interception.


### 4.2.6. Chain Emails

Users must not forward chain mails, advertising materials, photos, videos or any other content related to entertainment to another person using official emails.

### 4.2.7. Automatic Forwarding

Users should not automatically forward their official e-mails to any email address outside the government organization's networks. Forwarding mails, copying or blind copying official emails to email addresses outside the organizations network is prohibited. Automatic forwarding of e-mails within the government organization for business purposes may be allowed with the prior approval of designated personnel of the government organization.

### 4.2.8. Disclosing Email Address

Users must not publish or distribute internal mailing lists to non-staff members. If an employee is required to share an email address of another employee for official purposes, the employee who intended to share email should obtain the approval of other and the relevant authority for sharing such information with a third party.

### 4.2.9. Digital Signature

Users are recommended to use a digital signature to provide assurance to the receiver of the email. Refer Chapter Cryptographic Control Chapter for Digital Signature.

## 4.3. Safe and Appropriate Use of Internet and Social Media

### 4.3.1. Sending Information over Internet

Users must not release organization's information over the Internet without formal approvals from the authorized officers. Further, users must not place government organization material (software, internal memos, etc.) on any publicly accessible Internet computer.

### 4.3.2. Reporting Suspicious Activities

Users are instructed to report any suspicious activity, questioning or contact when using the Internet to the Incident Response Team.

### 4.3.3. Appropriate Content

While using Internet resources provided by the government organizations, users must not download or upload entertainment content or content that may be disruptive, harmful or offensive to others, or downloading of politically sensitive material or obscene content.

Users are required not to disclose information derived as a result of their access to information systems of organizations to unauthorized parties.

### 4.3.4. Privacy Setting on Websites

Users will be encouraged to use privacy settings for websites to restrict access to their personal information only to those they authorize to view it.

### 4.3.5. Posting Content on Websites

Users need to take special care not to accidentally post information on websites, especially in forums and blogs when official information infrastructure is used. Users must be made aware that even official information classified as unclassified that appears to be benign in isolation could, in aggregate, have a considerable security impact on the organization or government sector or wider government.

User need to be aware that any personal interest or other information they post on websites can be used to develop a detailed profile of their families, lifestyle, and interest in order to attempt to build a trust relationship with them. This relationship could then be used to attempt to elicit information from them or implant malicious software on systems by inducing them to, for instance, open emails or visit websites with malicious content – NISM

*Box 4C*

### 4.3.6. Bypass Security Controls

Users must not attempt to bypass the monitoring system of the organization by installing or using software that bypasses the Internet filtering system or through any other method. Users must also not install any devices to directly access Internet other than devices provided by the government organization.

### 4.3.7. Social Media Usage

Users should not use social media during office hours using the resources of the government organization. Organizations must ensure that users are informed of the security risks associated with posting personal information on websites or social media, especially for those personnel holding higher level security clearances.


### 4.3.8. Peer-to-Peer Information Sharing

Peer-to-peer communication tools have the ability to scan the entire computer system and can share files with peers or for public consumption automatically. Users of government organizations, therefore, should not use such applications.

### 4.3.9. Right-to-Audit

All the sites that users access through the government organization's network will be recorded to monitor the usage patterns of the users. Government organization may choose to monitor compliance with aspects of web usage policies, such as access attempts to blocked websites, pornographic content, entertainment websites, and gambling websites, as well as compiling a list of system users that excessively download and/or upload data without an obvious or known legitimate business requirement.

# 4.4. Safe and Appropriate Use of Mobile Devices

## 4.4.1. Connecting Unauthorized Devices

Users should not connect any unauthorized devices such as external disk, flash disk, mobile phones or other mobile devices to devices supplied by the organization without obtaining approval from the ISO.


## 4.4.2. Protection of Devices

Users must be aware that the Mobile Computers supplied by the organization contain organizational data, and therefore, take appropriate action to protect the device from being lost or stolen or from unauthorized access. The mobile computing devices shall include Laptops, Tabs, Mobile Phones, or other devices that are used to process data.

## 4.4.3. Protection of Devices

Users shall not connect organization supplied mobile devices to third party infrastructure.

## 4.4.4. Connect to Wifi-Networks

Users shall not access internet through third party Wi-Fi networks (or public Wi FI) by using official infrastructure or devices. Accessing such networks should be done only when absolutely required and properly authorized.

## 4.4.5. Change Security Settings

Users are not authorized to change any device security settings, or install software or programs without prior approval from the ISO.

### 4.4.6. Repairs to Devices

All the repairs or maintenance activities of the organization supplied mobile devices should be done only by the organization. Users should not directly handover mobile devices to any party outside the organization for repairs or maintenance.


### 4.4.7. Share Devices with Others

Users must not share organization supplied mobile devices with other staff or family members.

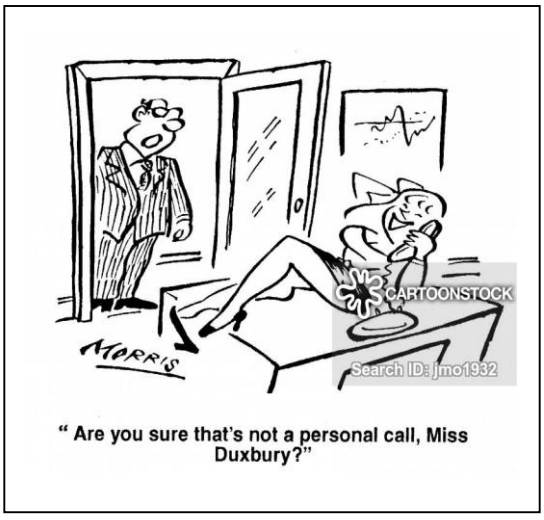
## 4.5. Safe and Appropriate Use of Telephones

### 4.5.1. Accountability of Telephone Calls

Employees are responsible for all calls made on office phone, and for the safe-keeping of the phone.

### 4.5.2. Phones for Personal Communication

Employees shall refrain using office phones for personal communications. Personal mobile phones generally should not be used for organization-related purposes unless an organization-provided phone is not available.




### 4.5.3. Photographing Secure Areas

Photographing secure areas and data processing facilities through mobile phone in the organization is prohibited.

### 4.5.4. Protecting Sensitive Information

Employees should not reveal sensitive or classified information over the telephone unless the telephone lines have been specifically secured for this purpose, for example, through the use of encryption.

### 4.5.5. Storing Information

Storing confidential messages, documents and any information asset owned by the organization unauthorized in personal devices is strictly prohibited.

### 4.5.6. Recording Calls

All parties to a telephone call must be notified in advance if the call is to be recorded.

## 4.6. Safe and Appropriate Use of Fax

### 4.6.1. Fax for Personnel Communication

Employees must not use office fax for personal communications

### 4.6.2. Sensitive Information over Fax

Sensitive or confidential information must only be faxed where a more secure means of communication is not available. Both the sender of the information and the intended recipient must authorize the transmission of the information before the transmission.

### 4.6.3. Unintendant Recipient

All fax messages should include a confidentiality clause prohibiting the recipient from disclosing the information if such a fax is received by error. Any fax received by error must be destroyed and its sender should be notified if possible.

# Notes