©(ORGANISATION NAME)

EMAIL POLICY

Subject: Email Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 14	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 OVERVIEW

Electronic mail (email) simply put, is the transmission of computer-based messages – text, images, forms, attachments, data, or other communication over telecommunication channels. Email systems are used to send, receive, and store messages, including attachments where applicable. At the same time, misuse of email can create legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

1.1 RISKS ADDRESSED

The following are the risks associated when communicating with emails:

Reference	Description of Risk
SAFETag	Lack of proper encryption both At Rest and In-Transit
SAFETag	Email Interception
SAFETag	Phishing Attacks: Links in emails can also contain malwares

1.1 PURPOSE

- To establish guidelines and procedures for the proper use of Organisation's email system and make users aware of what the Organisation considers acceptable and unacceptable uses of the email system.
- To establish the criteria governing the authorised use of personal or corporate owned smartphone and tablet (mobile) devices where the owner has established access to the Organisation's email systems enabling them to send or receive work related email messages and conduct other Organisation business.
- To raise awareness of the security risks associated with the use of personal email for official purposes and thus any official email must be communicated through Organisational domain and not the use of personal email such as abc@gmail.com, abc@yahoo.co.uk, these should not be used for official purposes.
- To have knowledge about do's and don'ts of using an Organisation's email and the need to implement SSL/TLS encryption for the Organisation's email server.

1.2 OBJECTIVES

The objective of this policy is to ensure that:

- The need for secure email usage is communicated effectively.
- The Organisation's email assets and information facilities are adequately used.

1.3 SCOPE

This policy applies to management, all employees, and third parties operating on behalf of the Organisation and covers appropriate use of any email sent from an Organisation email address.

1.4 RELATED DOCUMENTS

The following policies and procedures are relevant to this document:

- Password Policy

2. POLICY DETAILS

2.1 GENERAL

- All email accounts maintained on the Organisation's email system are property of the Organisation and are primarily provided for official purposes.
- Extensive use of email privileges for personal purposes is considered a violation to this policy; only limited personal use of the Organisation's email system is permitted. Personal use of the email system must not interfere with normal business activities, must not involve solicitation, must not be associated with any profit outside business activities or any potential embarrassment to the Organisation.
- The standard client for email access in the Organisation shall be Microsoft Outlook and OWA.
- Users who receive confidential information accidentally shall notify the sender and delete such email immediately.
- Attachment of data files to email shall only be permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.
- All users on the Organisation's email platform shall be provided with unique email addresses. The email addresses shall be constructed in line with the following naming convention: firstname.surname@Organisation.com However, where there are conflicts (e.g., where two or more staff have similar first and last names) the middle name shall be included to differentiate firstnamemiddlename.surname@Organisation.com
- Information Technology is responsible for the administration, maintenance, and operation of the Organisation's email system, including the messages stored or transmitted through it. Except by management approval, IT does not have the right to view, delete, or in any other way, modify users' email messages.

- Email accounts are to be used only by the authorised owner of the account name. Account owners shall be held responsible for all activities performed through their account.
- Users accessing their emails from public facilities, e.g., cyber cafes, must exercise due care to ensure that the Organisation's information is not by any means revealed to unauthorised persons.
- Users must not employ any electronic email addresses other than official electronic email addresses for Organisation' s business messages. Where official electronic mail addresses are unavailable, management approval must be sought before other email addresses can be used for official communication.
- Users must verify/validate the correctness/appropriateness of email addresses to ensure that Organisation' s emails are not sent to unauthorised recipients.
- Broadcast of technical information to all staff shall be permitted for some teams using specialised email accounts as the need arises. However, other staff whose job functions require them to send emails to all staff of the Organisation shall require management approval.

2.2 PROHIBITED USE

- Use of an email account assigned to another individual, whether to send or receive messages, shall require prior approval, such as when accessing a staff member's email during their absence (e.g., vacation).
- Forwarding of documents, records and email correspondence deemed confidential and sensitive to third parties outside the Organisation network without the written consent of the Head, Legal Services or designate.
- Unauthorised modification or alteration of email messages. Such modification includes forging and removing information appearing anywhere in an email message including the body of the message or the header (this applies to email trails also).
- Initiating or forwarding chain emails or spam from any Organisational email account or computer system, or any device used to access the Organisation's information asset. Any user that discovers spam in the Organisation or associated with the Organisation's email should report to the IT Service desk immediately for appropriate action.
- Opening of email attachments from unknown or untrusted parties. Such attachments must be deleted immediately or forwarded to the IT Help Desk for investigation.
- Transmission of copyrighted materials via the Organisation's email system without appropriate permission.
- Using the Organisation's email systems to distribute, disseminate or store indecent, disruptive, discriminatory, or harassing materials. Such materials include comments

about race, religious and political beliefs, pornography, hoaxes, etc. Employees who receive such email messages from any staff of the Organisation should report to Human Resources immediately.

- Any other use of the email system in a way that violates the requirements of the Organisation's policies.
- Monitoring of email messages passing through the Organisation's email system without management approval.
- Forwarding of emails containing the Organisation's sensitive information outside the Organisation's network (i.e., to third parties) without management approval.
- Sending Of Anonymous Or pseudonymous emails to any recipient.

2.3 MONITORING

- The Organisation is committed to protecting user privacy. However, management reserves the right, employing any preferred means, to monitor, read and keep record of the content of all email transmitted on the network using the email system. Organisation emails are subject to monitoring for the following reasons:
    - Policy adherence
    - Security purposes
    - Legal obligation
    - Auditing
    - To detect unauthorised use

- Electronic email messages flowing through the Organisation systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons. In the same vein, the content of email messages may be disclosed to law enforcement officials without prior notice to the staff that may have sent or received such messages.

2.4 MOBILE DEVICE EMAIL USAGE

- The usage of email on mobile devices must comply with the Organisation's overall Email security policy.
- Users using mobile devices to access the Organisation's email shall be responsible for the protection of the Organisation's information on these devices.
- Users are responsible for ensuring the operating systems on their mobile devices are updated regularly.
- Users are responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread – Please refer to the Antivirus Policy.

- Devices used to access the Organisation's email must at a minimum be protected by passwords/passcodes and these passwords /passcodes must have a minimum length of 4 characters.
- Users are prohibited from copying sensitive data from email applications to other applications on the device or to an unregistered personally owned device.
- Devices used to access the Organisation's email must not be given out (sold, given as gift to non-staff members, etc.) without first notifying the IT Service Desk.
- Users using their mobile devices to access official emails must always ensure adequate physical protection of the devices; such devices must not be left unsupervised.
- Devices that are lost or stolen or are believed to have been compromised in some way, must be reported immediately to the IT Service Desk so that email access can be deactivated.
- The Information Security Unit reserves the right to carry out spot checks of the configuration of devices used to access official email to ensure compliance with the requirements of this policy.
- The Organisation reserves the right to block email access, remote wipe of Organisation content or reset to factory settings on the registered mobile device.

2.5 EMAIL BACKUP, RECOVERY AND AVAILABILITY

- Backup tapes created by Information Technology shall solely be for the purpose of restoring the email system in the event of disaster. These tapes may not allow for restoration of individual mailboxes and cannot be used as a convenience to retrieve "deleted" messages.

- Backups do not replace records retention; they are requirements for disaster recovery. Each user must make provisions to retain messages in accordance with applicable Organisation, department, regulatory and legal records retention provision.

- Information Technology shall make all efforts to ensure availability of the email systems; these efforts include providing email processing systems at alternate locations.

2.6 SENDING AND RECEIVING EMAIL

Users must understand that all the organisation's emails are the organisation's property and must not use Organisation's email to sign up for accounts not related to work. All outgoing emails containing sensitive information must be encrypted to avoid breach of confidentiality and integrity of data.

Users should also be aware of phishing emails because links in the emails can contain malwares. Before we dive into ways to identify phishing emails, let's define what Phishing Emails/Attacks are.

2.6.1 Phishing Email:

Phishing is a fraudulent practice in which an attacker masquerades as a reputable entity or person in an email or other form of communication to steal sensitive information such as login credentials, financial details, usernames, and other personal information from victims.

Step by Step Guide to Identify Phishing Emails:

- **Urgent call to action or threats**: Be wary of emails that demand immediate action, such as clicking a link, making a call, or opening an attachment. These often claim you must act now to claim a reward or avoid a penalty, such as a suspended account that requires unlocking. This sense of urgency is a common tactic in phishing attacks and scams, intended to prevent thoughtful consideration or consultation with a trusted advisor. Figure 1 shows an example of this, with an urgent call to action about training ending soon and a 7-day enrolment window. The challenge is that the recipient had already completed the ISC2 modules and passed the exam in November 2023, making the email's claims seem more plausible.

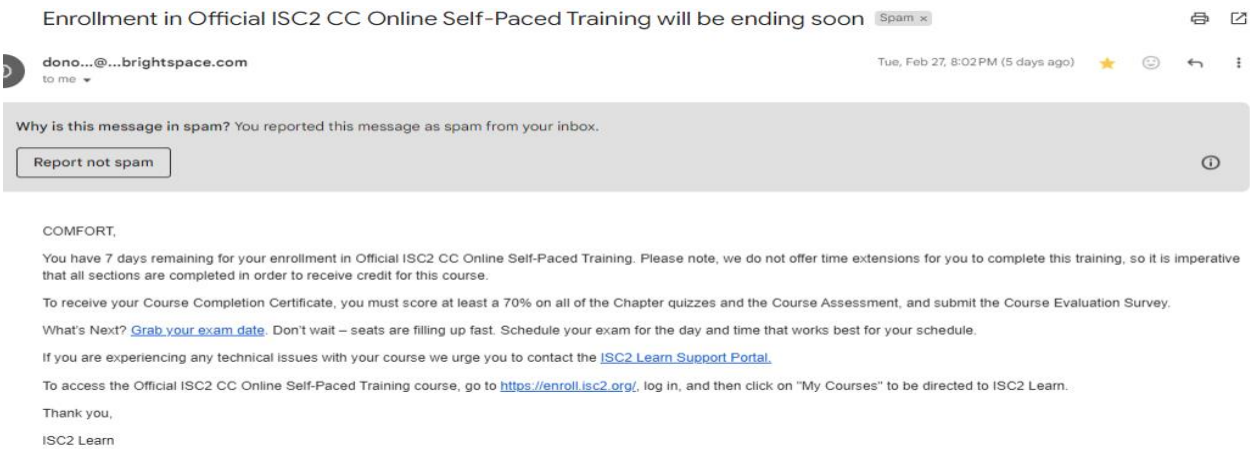
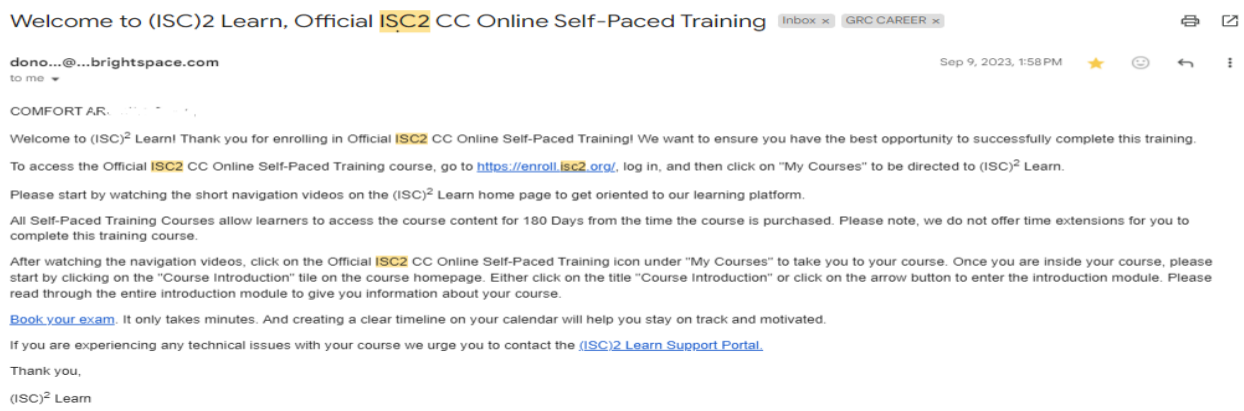


Fig 1: Fake Email



Welcome to (ISC)2 Learn, Official ISC2 CC Online Self-Paced Training Inbox × GRC CAREER ×

dono...@...brightspace.com Sep 9, 2023, 1:58 PM
to me

COMFORT AR...

Welcome to (ISC)² Learn! Thank you for enrolling in Official ISC2 CC Online Self-Paced Training! We want to ensure you have the best opportunity to successfully complete this training.

To access the Official ISC2 CC Online Self-Paced Training course, go to https://enroll.isc2.org/, log in, and then click on "My Courses" to be directed to (ISC)² Learn.

Please start by watching the short navigation videos on the (ISC)² Learn home page to get oriented to our learning platform.

All Self-Paced Training Courses allow learners to access the course content for 180 Days from the time the course is purchased. Please note, we do not offer time extensions for you to complete this training course.

After watching the navigation videos, click on the Official ISC2 CC Online Self-Paced Training icon under "My Courses" to take you to your course. Once you are inside your course, please start by clicking on the "Course Introduction" tile on the course homepage. Either click on the title "Course Introduction" or click on the arrow button to enter the introduction module. Please read through the entire introduction module to give you information about your course.

Book your exam. It only takes minutes. And creating a clear timeline on your calendar will help you stay on track and motivated.

If you are experiencing any technical issues with your course we urge you to contact the (ISC)2 Learn Support Portal.

Thank you,

(ISC)² Learn

Fig 2: Original Email during the training. You can spot the difference between Fig 1 and Fig 2

- **Hover before you click:** If you suspect that an email message is a scam, *don't open any links or attachments* that you see. Instead, hover your mouse over, but *don't click* the link. Look at the address that pops up when you hover over the link and check if the address matches the link that was typed in the message. In Fig 3 below, resting the mouse over the link reveals the *real* web address in the box with the yellow background. The string of numbers looks *nothing like* the company's web address.

Fig 3.

- **Generic greetings**: If the email starts with a generic "Dear sir or madam", "only first name", "to whom it may concern," "dear customer", that's a warning sign that it might not be genuine because a professional organisation will rather address you by your first and last name just like Fig 2 above. Fig 4 below is an example of generic greeting in phishing emails.

Fig 4

- **Spelling and bad grammar:** If an email message has obvious spelling or grammatical errors, it might be a scam. Professional companies and organisations are very strict about email they send out and will avoid bad grammar in their emails.
- **Emails asking for personal information:** Beware of emails asking for personal information such as financial details, passwords, usernames, and Personal Identifiable Information (PII). Legitimate organisations will never ask for this over email.

2.7 WHAT TO DO IF YOU RECEIVE PHISHING EMAILS.

If you received a phishing email in your inbox, these are the following steps to follow:

- Never click any links or attachments in suspicious emails.
- If the suspicious email appears to come from a person you know, contact that person via another means like by text message or a phone call to confirm it.
- Report the suspicious email to the IT/Security team in your organisation.
- After reporting the suspicious email, it's safe to go ahead and delete it. In most email clients, deleting a message sends it to another folder labelled "trash" or "deleted items." If this is the case, navigate into that folder and delete it permanently.
- Never forward phishing emails or suspicious messages to your colleagues since they might click a link or download an attachment.

2.8 HOW TO AVOID PHISHING EMAILS OR SOLUTIONS TO PHISHING EMAILS:

- Implement a phishing filter to detect and block phishing attempts.
- Train employees to recognize phishing tactics.
- Use multi-factor authentication to add an extra layer of security.

While personal email services can be convenient for individual use, using an Organisation's domain email address is generally recommended for professional communication, as it offers advantages in terms of credibility, security, branding, and management.

3. MAINTAINING YOUR EMAIL ACCOUNT

- When maintaining an email account as per Organisation's email policy, you should take the following steps into consideration to stay compliant:
- Staying within permitted mailbox sizes is also essential to avoid overloading Organisation servers and ensure cost-effective use of the email. First, review the retention policy thoroughly and set up archiving and auto-deletion rules accordingly. Any guidelines around keeping or deleting emails after a defined period should be followed diligently.
- Follow security protocols like enabling two-factor authentication and avoiding auto-forwarding Organisation emails to personal accounts. Such measures restrict access and prevent potential data leaks. In addition, encrypting sensitive emails ensures customer and Organisation information stays protected.

- Ensure you adhere to password policy, creating complex security credentials for your email and changing them at regular intervals as mandated. Furthermore, allowing third-party apps or services access to the Organisation email should only be done after careful consideration, as this can risk data leakage if proper vetting isn't done.
- Reading through updated versions of the email usage policy and informing IT teams of any potential compliance or security risks is crucial.

4. EMAIL ENCRYPTION TOOLS

Below are the free applications software for sending and receiving encrypted emails or messages:

- GPGTools
- Mailvelope
- GNU Privacy Guard
- AnonEmail
- Proton
- Infoencrypt
- Enigmail
- Mymain Crypt for Gmail
- Gpg4Win

5. RECOMMENDATIONS/ADVISORY ON EMAIL POLICY

Based on the importance of using an Organisation's domain email address for professional communication, the recommendations are split into two categories based on the number of employees in an Organisation.

CATEGORY A: FOR 1-5 NUMBER OF EMPLOYEES IN AN ORGANISATION:

- ★ Register your domain (e.g., abc.com)
- ★ Host your domain.

Below are the top 3 companies for hosting your domain with a link to their site.

1. Namecheap: Click here for the link
2. GoDaddy: Click here for the link
3. Bluehost: Click here for the link

When you host your domain on any one of the above hosting companies, you will have access to unlimited emails, if you don't bother much about additional services because you are small and just coming up.

CATEGORY B: FOR 5-20 NUMBER OF EMPLOYEES IN AN ORGANISATION:

- ★ Register your domain.
- ★ Subscribe to email service providers.

If you don't want to continue with the email services of your domain provider, then subscribe to any of the following email service providers.

1. Google Workspace: Click here for the link
2. Microsoft Office 365: Click here for the link
3. Zoho Mail: Click here for the link

If you have any questions about the above policies, please contact the IT Manager or Head of IT.