ACCEPTABLE USE POLICY

Subject: Acceptable Use Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 21	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. If 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

This document is the property of CcHUB. Circulation is restricted to the Organisation’s use. It must not be copied or used for any other purpose other than for which it is supplied, without the expressed written authority of CcHUB.

Except where provided for purposes of contractual requirements, CcHUB disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is addressable by CcHUB.

CONTENTS

1.0 INTRODUCTION

Information Assets are strategic assets of the Organisation and must be treated and managed as valuable resources. The Organisation provides various information assets to be used for business purposes in serving the interests of the Organisation, our clients and customers for business operations. This Acceptable Use Policy (AUP) is designed to protect the Organisation, our employees, customers and other partners from harm caused by the misuse of our information and information assets. As such, all employees and users must ensure they adhere to the guidelines in this policy. Managers are responsible for ensuring that all people working for the Organisation and using the company's information assets in any capacity, receive a copy of these policies, read them, and understand them. Every user is accountable for upholding the confidentiality, integrity, and accessibility of the Organization's information assets..

1.1 PURPOSE

This Policy is established to achieve the following:

- To establish appropriate and acceptable practices regarding the use of the Organisation's information assets
- To ensure compliance with applicable policies regarding the management of information resources.
- To educate individuals who may use information assets with respect to their roles and responsibilities.

1.2 SCOPE

This policy applies to all systems, individuals, and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to the organisation's systems.

1.3 OBJECTIVES

The objective of this policy is to protect the confidentiality and integrity of information and privacy of its customers and users.

2. ACCEPTABLE USE POLICY

2.1 EMAIL ACCEPTABLE USE

Electronic email is pervasively used in almost all industries and is often the primary communication and awareness method within an organisation. At the same time, misuse of email can pose legal, financial, reputational and privacy impacts for users, employees and organisations.

The purpose of this email policy is to ensure the proper use of Organisation email system and make users aware of what Organisation deems as acceptable and unacceptable use of its email system.

- Access to the Organisation’s electronic mail (email) system is provided to employees and/or third parties whose duties require email to perform their business as usual for the Organisation’s business operations.
- All messages composed and/or sent using Organisation provided electronic messaging resources must comply with Organisational policies regarding acceptable communication.
- The Organization strictly prohibits discrimination based on age, race, gender, sexual orientation, religious, or political beliefs. Any use of electronic messaging resources for discriminatory purposes related to any or all these factors is strictly forbidden.
- Upon termination or separation from the Organisation, users shall be denied all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Each employee shall be assigned a unique email address that is to be used while conducting Organisational business activities via email.
- Electronic messages are sometimes inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Since email may be monitored, all employees using the corporate email resource to transmit or receive email shall have no expectation of privacy.

- Messages, data, programmes, or files that could potentially cause hardware, software, or network failure and/or the destruction of data must not be transmitted or received.
- The Organisation prohibits staff from participating in "chain" emails, jokes or spending an inordinate amount of time organising non- Organisation-related social events via the email system. Whilst urgent emails to friends and family are sometimes unavoidable, employees must take care not to abuse the system.
- Attachments sent to external sources should be avoided unless they are business critical. Confidential or business sensitive emails and attachments should be password protected and/or encrypted.
- Receiving inappropriate emails may be unavoidable, but users are responsible for preventing the further spread of such inappropriate content. Any email containing unprofessional or unsuitable material should be deleted upon receipt. Forwarding such email is unacceptable.
- It is unacceptable to send persistent, aggravated, or intimidating emails to another person, whether a fellow employee or not.
- Email accounts assigned to one person should not be used by another unless they are given specific authorisation to do so. Where authorisation is provided, email forwarding or delegation facilities should be adopted.
- The use of "Generic" accounts to access email databases is not permitted unless authorised by the Organisation’s system administrator and approved by relevant authorities. All email activities must be traceable to an individual by name.
- Email messages must not be forwarded "automatically" using agents or forwarders to any external email address.
- Organisation’s internal emails should not be forwarded to external addresses, unless there is a specific business need. This is crucial when the messages contain confidential or sensitive information, especially if the external recipient is not bound by a confidentiality agreement.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct the organisation's business activities, to create or memorialise any binding transactions, or to store or retain email on behalf of the Organisation. Such communications and transactions should be conducted through proper channels using the Organisation's approved email platform.
- The Organisation's email address should NOT be used to subscribe to any non-business-related sites or materials.
- Any employee who discovers a violation of these policies should immediately notify the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

2.2 EMAIL FLOW CONTROL LIMIT

Organisation's Email Service imposes various limits and automatic restrictions to serve as a preventive control for its users and the organisation. These limits are implemented to safeguard against malicious and accidental abuse of the system. Example of such limits include (among others):

Maximum message size = 10mb

Number of emails an account can send or receive per unit of time.

For email with attachment(s) greater than 10mb, such attachment(s) should be placed on the Organisation's intranet portal or shared drive and the link should be shared with the intended recipient.

2.3 PROHIBITED USE

Prohibited activities when using the Organisation's email include, but are not limited to sending or arranging to receive the following:

- Information that violates State or Federal laws or the Organisation's policies.

- Information designated as confidential or sensitive unless encrypted according to the Organisation's standards.
- Unsolicited commercial announcements or advertising material.
- Any content that could defame, abuse, embarrass, tarnish, present a negative image of, or portray in a false light the Organisation, the recipient, the sender, or any other person.
- Pornographic, sexually explicit, or sexually oriented material.
- Racist, hate-based, or offensive material.
- Viruses or malicious code.
- Chain letters unauthorised mass mailings, or any unauthorised request asking the recipient to forward the message to other people.
- Circulating, spreading, or disseminating information to email groups which the user has not been designated or authorised to communicate.

2.4 AUTHORISED MONITORING

IT Support Staff with unrestricted access to data, email, and similar services must receive management approval from/through the Head of IT, prior to decrypting or reading the email traffic of employees or third parties.

2.5 OWNERSHIP

- The email/electronic messaging systems are an Organisation's property. All messages stored in the Organisation's provided electronic messaging system(s) or composed, sent, or received by any employee or non-employee belongs to the Organisation.
- Electronic messages generated, processed, or terminated on the Organisation's information systems/infrastructure are NOT the property of any employee.
- The Organisation reserves the right to intercept, monitor, review and/or disclose all emails/messages generated, transmitted, or stored.
- The Organisation reserves the right to alter, modify, re-route, or block the delivery of messages as appropriate. Especially if it poses a threat or risk to the organisation.

- The unique email addresses assigned to an employee are the property of Organisation.
- Users are not allowed to delete any Organisational information from the official computer systems without justification or management's approval.

2.6 EMAIL SIGNATURE POLICY

- Employees may not create their own variations or interpretations of the official email signature style for outgoing emails. Employees may not add other information, including links to other websites or social media accounts, to their official email signature.
- They may, however, create a secondary, condensed version of the email signature to use for replies/forwards, providing (at minimum) their name, the name of Organisation, and a phone number, when sending official emails from a mobile phone.
- No mottos, quotations, taglines, or other statements may be added to the approved email signature, as these could be misunderstood as representing the Organisation's official positions, values, or views. No borders, backgrounds, photos, GIFs, emojis, logos or other images may be used in conjunction with the Organisation's official email signature.
- Once an employee has an approved email signature consistent with current brand standards of the organisation, older email signatures should be deleted so they are not used inadvertently.
- All job titles used on official email signatures must be approved by the HR Department and must be in-line with official job titles as stated in the employment letter.

2.7 AUTO-FORWARDING OF EMAIL

Employees must exercise utmost caution when sending any email from the Organisation's network to an external network. Sensitive information should not be forwarded via any channel, unless such email is critical to business and is encrypted.

Manually forwarding the Organisation’s email that contains information classified as confidential is only permissible for justified business purposes and appropriate security precautions such as email encryption must be used.

The use of automation tools such as auto-forwarding, POP, IMAP etc., to move email from an email system managed by Organisation is only permissible with approval from management and IT team must be consulted.

2.8 INTERNET USAGE

The Internet must only be used to obtain information that is key to the performance of an employee’s role within an organisation. Access to the Internet from the Organisation owned device can only be conducted through secured and approved connection methods. Internet access shall be granted only to employees, contractors, subcontractors, and business partners whose duties require such access to conduct the Organisation’s business operations, subject to prior approval. Since Internet activities may be monitored, all users accessing the Internet using the Organisation’s resources shall have no expectation of privacy.

The Organisation prohibits employees from using the Internet and its infrastructure for unofficial purposes such as but not limited to:

- Accessing websites for personal interest (recreational browsing)
- Searching Internet job sites
- Using the Internet for inappropriate personal use
- Other online activities that impacts other employees productivity

2.9 ACCEPTABLE USE

The organisation shall provide internet access to facilitate the conduct of its business operations. Occasional and incidental personal Internet use is permitted if it does not interfere with the employee’s work or of the Organisation’s ability to perform its mission and it meets the conditions outlined in the Organisation’s policies and procedures.

2.10 PROHIBITED USE OF THE INTERNET SERVICE

Except where it is strictly and necessarily required for work responsibilities, such as IT audit activities or other investigations, you must **not** use your Internet access provided by the Organisation to:

- Browse explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the Organisation has determined to be off limits.
- Post, send, or acquire sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material determined to be off limits by the Organisation.
- Post or send classified Organisation’s information outside of the Organisation’s network without management authorisation.
- Hack or perform other unauthorised use of services available on the Internet.
- Post unauthorised commercial announcements or advertising material.
- Promote or maintain a personal or private business.
- Receive news feeds and push data updates unless the material is required for the Organisation 's business.
- Use unauthorised and unapproved applications or software that occupy or use workstation idle cycles or network processing time (e.g., processing in conjunction with screen savers).
- Use the Organisation’s equipment for inappropriate personal use.
- Use the Internet for any act that violates local status, laws, or regulations, inclusive but not limited to duplication or dissemination of copyrighted materials and trade secrets.
- Maliciously tamper with any computer system to disable, defeat or circumvent any security systems put in place to monitor and control activities on the Internet.
- Refer to the Organisation, its products, services, customers, potential customers, or personnel in any unofficial, published websites, blogs or otherwise make statements that could damage the reputation of the organisation or another party.
- Scan and print non-official documents.

- Perform Cyber-crime activities or Gamble.
- Subscribe to, enter, or use peer-to-peer networks or install software that allows sharing of music, video, or image files.
- Subscribe to, enter, or utilise real time chat facilities such as chat rooms, text messenger or pager programs that are non-business related.
- Subscribe to, enter, or use online gaming or betting sites.
- Download any software that does not comply with the organisation's Software Policy.

The above list provides examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material would include data, images, audio files or video files whose transmission is illegal as well as material that violates the rule, essence and spirit of this policy and other organisation policies.

The organisation will take steps to block the following categories of websites:

- Illegal.
- Pornographic.
- Violence.
- Hate and discrimination.
- Offensive.
- Weapons.
- Hacking.
- Web chat.
- Gambling.
- Dating.
- Radio stations.
- Games.
- Streaming Media.

If you have inadvertently attempted to access such a site, you should inform the ICT Department immediately.

2.11 GENERALLY PROHIBITED USE OF INFORMATION RESOURCES

Generally prohibited activities when using the Organisation's information resources include, but are not limited to, the following:

- Using mobile devices connected to the Organisation's network without the use of an appropriate authentication or locking mechanism e.g., passwords. Passwords used on such mobile devices (mobile phones, tablets etc.) shall comply with the Organisation's Password Policy.
- Mechanisms shall be provided to protect devices against malware, remote disabling, usage of web services, encryption, software installation and access control over mobile devices used within the organisation's network.
- Ensuring information resources (computers, servers, laptops, hard drives, USB drives, etc.) are not left unattended. Sensitive or critical business information on paper or electronic media must be securely stored when not in use.
- Leaving equipment and media containing Organisation's data unattended in public places. Employees are responsible for ensuring the physical security of Organisation's information resources when taking them off the premises.
- Distribution of media amongst employees and systems via the use of USB flash or any other removable drive is prohibited unless approved for official business purposes.
- Stealing electronic files or copying of electronic files not related to normal business activities without management approval.
- Violating copyright laws.
- Installing unauthorised software, including games and screensavers.
- Browsing the private files or accounts of others, except as provided by appropriate authority.
- Performing unofficial activities that may degrade the performance of information resources, such as playing electronic games.

- Performing activities intended to circumvent security or access controls of any organisation, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt or encrypt files or compromise information security by any other means except if authorisation is given.
- Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any Organisation's computer, network, or information.
- Promoting or maintaining a personal or private business or using Organisation's service information resources for personal gain.
- Using someone else's logon ID and password.
- Conducting fraudulent or illegal activities, including but not limited to: gambling, drugs or weapons trafficking, participating in terrorist acts, or attempting unauthorised entry to any Organisation's computer.
- Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.
- Disclosing any Organisation's information that is not otherwise public without authorisation or management approval.
- Performing any act that may discredit, defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray the Organisation's staff, business partners, or customers in a false light.

2.12 CLEAR DESK AND CLEAR SCREEN

2.12.1 INTRODUCTION

To improve the security and confidentiality of information, all staff should adopt a clear desk policy for physical documents and removable storage media, as well as a clear screen policy for computer monitors, whenever possible.

This measure is intended to reduce the risk of unauthorised access, loss of data, and damage to information during and outside normal working hours, or when work areas are unattended.

Organisational clear desk & clear screen policy are stated in the sections below. Staff are always required to adhere to the following directives.

- Sensitive or critical business information, whether in physical documents or electronic storage media, shall be securely kept away (ideally in a safe cabinet or other secure furniture) when not in use, especially when the office is vacant.
- Computers and terminals shall be logged off when unattended and should have security measures enabled to protect them when not in use, such as passwords.
- Media or devices containing sensitive or classified information shall be removed from printers immediately.

2.12.2 WORK ENVIRONMENT

- Maintaining a neat work environment during and after business hours, ensuring all sensitive and unnecessary materials are cleared from the desk.
- Taking time to clear accumulated paperwork at regular intervals, e.g., once a week.
- Avoid cluttering the work area with handwritten notes and sticky notes displaying sensitive information.
- Avoid writing down passwords, User IDs, or account information.
- All evidence of previous meetings, notes on paper, whiteboards, computer screens or flip charts should be removed from sight before a customer or supplier enters a meeting room.
- Ensuring that no confidential information is left in in-trays or exposed areas outside of office hours.
- Ensuring the reception desk areas are always cleared; customers, suppliers or project details should not be kept on the desk within reach/sight of visitors.
- Ensuring all information is securely stored in departmental cabinets or lockers with restricted access. This practice helps prevent information from being exposed, as well as reducing the risk of data being damaged or destroyed in the event of a disaster such as fire, flood, or explosion.

2.12.3 INFORMATION HANDLING AND PRINTING

- Ensuring all documents obtained from other departments should be promptly returned when no longer needed.
- Only print necessary information on paper and avoid printing when not needed.
- Printers should have authentication methods such as individual PINs or password before documents sent to printers can be released/printed.
- Removing confidential or internal information from printers immediately.
- Removing documents from scanners, photocopiers, printers, and fax machines as soon as they are scanned, copied, or printed; this helps ensure that sensitive documents are not left in the device trays for an intruder to pick up.

2.12.4 STORAGE OF INFORMATION

- Ensuring photocopiers are switched off and locked (where possible) outside working hours; this makes it difficult for unauthorised copying of sensitive information.
- Ensuring paper including letter headed paper and other Organisational branded paper and computer media are stored in suitable locked safes, cabinets, or other forms of secured furniture when not in use, especially outside working hours (where practically possible).
- Ensuring office / room doors are locked and not left unattended in order to prevent unauthorised access (this is to safeguard lockable safes, filing cabinets, drawers, cupboards etc.).
- Ensuring all sensitive information and objects are removed from the workplace and stored in a locked area at the end of each day, or when away from the work area for an extended period.
- Ensuring all Organisational information assets and customer information are properly secured in a fire-resistant cabinet. Physical documents may be scanned and filed in electronic format with adequate backup available.
- Ensuring portable computing devices such as laptops are stored in a locked area at the end of each day, or when away from work area for an extended period.

- Ensure keys to locked safes, cabinet, office doors are retrieved and safely kept to restrict access to them.

2.12.5 CLEAR SCREEN GUIDELINE

- Ensuring computers are not left logged-on when unattended and ensuring that they are password-protected.
- Ensuring computer screens are angled away from the view of unauthorised persons.
- Ensuring the screen is set to automatically lock when there is no activity for a period of 3 to 5 minutes.
- Ensuring that after the screen locks, password entry is required.
- Ensuring machines are logged off when leaving the room or the office, particularly at the close of business every day.
- Ensuring personal computers are switched off when not in use and are password protected.

2.13 DISCIPLINARY ACTIONS

DISCIPLINARY ACTIONS - INFORMATION TECHNOLOGY

	Offences	**1st time - Stage One**	**2nd time - Stage Two**	**3rd time - Final**
Email	Illegal or unlawful use of email (copyright infringement, obscenity, libel, slander, fraud, defamation, intimidation, forgery, impersonation)	Summary Dismissal	N/A	N/A
	Sending email attachments internally where the Portal is available (in accordance with the paperless office drive)	Verbal warning	Query & written warning	1-month suspension
	Auto forwarding or moving emails from Organisation to personal account.	2 weeks suspension	Summary Dismissal	N/A
Internet	Internet misuse – pornographic site visit, downloads of malicious file types (movies, audio, etc. that are virus-infected)	Summary Dismissal	N/A	N/A
Information Resources	Deleting of business information or copy without authorisation or approval	Query & written warning	2 weeks suspension	Summary Dismissal
End user Hardware.	Deliberate Hardware misuse that may result in physical damage	Query & written warning	2 weeks suspension	Deduct certain amount from employee salary
	Hardware theft	Summary Dismissal	N/A	N/A

	Using the Organisation’s VOIP for personal use	Verbal Warning Deduct excess amount from employee salary	Query & Written warning. Deduct excess amount from employee salary	1-month suspension Deduct excess amount from employee salary
Accounts Management	Sharing passwords to Organisation applications with colleagues, family members, etc. (Email, business application, Network access, database. Etc.)	3 month’s suspension	Termination	N/A