University of Moratuwa
Information and Communication Technology Policy

1.0 Purpose

The University of Moratuwa (UoM) recognizes the vital role Information Communication Technology (ICT) plays in the University's academic, research, and administrative missions, as well as in communicating our work with staff, students, alumni, government, and business partners. The University recognizes that global access to information provides many opportunities, as well as the importance in an academic environment to protect the ICT facilities and information in all forms. As more information is created, used, and shared in digital form by students, faculty, and staff, an increased effort must be made to acquire fitting IT resources of the highest standards, as well as to protect all the ICT facilities that support such initiatives. Increased protection of our data and ICT facilities to assure the usability, reliability, and availability of those facilities is the primary purpose of this Policy. The secondary purpose of the policy is to align the University's ICT infrastructure, architecture, and operational activities with the industry best practices.

This Policy applies to all members of the University community and those who use University ICT facilities. When decisions are made regarding the acquisition and management of ICT infrastructure, architecture, and operational activities, the decision maker should consult this Policy for guidance.

2.0 Introduction

2.1 Principles

Following general principles applicable to a University environment is considered while preparing and executing this Policy:

1. Academic freedom – Academic freedom is a fundamental University value. This Policy will be administered in a manner that supports the principle of academic freedom.
2. Supportive academic environment – The University seeks to provide supportive learning, working, and living environment to the UoM community. Thus, we actively look for ways to bring together students, faculty, and staff, and to build a community that encourages all of its members to succeed and grow.
3. Accountability for University resources – All members of the UoM community have a responsibility to protect the University facilities for which they have access or custodianship. All members of the UoM community and external users are accountable for their access to and use of the University facilities.
4. Personal use – The University recognizes that students, faculty, and staff have reasonable expectations of privacy in their use of ICT facilities. However, rights to privacy are constrained in the University environment as (a) the University owns and

supplies these ICT facilities, (b) UoM ICT facilities contain many shared environments and facilities where the rights of other users must be considered, and (c) legal and ethical restrictions need to apply. Facilities owned and maintained by the University for the benefit of the academic community are primarily intended for the use of academic, research, administrative, and approved project activities, and not for personal, recreational, or business communications. Relevant policy conditions and constraints are defined under the "Acceptable Use Policy" and "Privacy Policy".

5. Relationship to departmental ICT policies – Departments, divisions, and projects within the University may adopt additional ICT policies that are specific to their operations, provided that such requirements are consistent with this Policy and copies of the unit-specific policies are provided to the Director, Center for Information Technology Services (CITeS). In the event of inconsistency, the provisions of this Policy will prevail, unless it is superseded by more specific policies that meet and governs legal requirements, in which case, the more specific legal requirements and related policies will take precedence.

2.2 Scope

This Policy applies to all internal and external users of the UoM ICT facilities. For the interpretation of this Policy users and ICT facilities are defined as follows:

1. Users – This Policy applies to everyone who accesses the UoM ICT facilities, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, consultants, temporary employees, guests, volunteers, and contractors. More specifically for:
    a. Internal students with a valid registration, either full-time or part-time
    b. Staff in current employment with the UoM, either permanent or contract
    c. Personnel of the UoM departments, divisions, projects, etc., with a valid authorization for the use of ICT facilities given by the Head of the relevant unit
    d. External users with a valid authorization for ICT facilities use given either by the Head of the relevant unit or CITeS

2. ICT facilities – for purposes of this Policy include, but are not limited to, University-owned personal computers, servers, computer peripherals, storage, services, software, wired and wireless networks, Internet connections, transmission lines, and exchanges. ICT facilities include those owned by the University and those used by the University under license or contract, including but not limited to, information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. ICT facilities also include, but is not limited to, personal computers, servers, computer peripherals, storage, wired and wireless networks, and other devices not owned by the University, but intentionally connected to the University-owned ICT facilities while so connected.

By accessing University ICT facilities, the user agrees to comply with this Policy.

The primary aim of this Policy is to protect and ensure the continuity of the University's ICT facilities and the information stored on them. The second aim of the Policy is to align the University's ICT infrastructure, architecture, and operational activities with the industry best practices to ensure only the compatible ICT facilities of the highest standards are

provided. Therefore, this Policy also applies to all current and planned ICT infrastructure, architecture, and operational activities by the UoM. The third aim of the Policy is to raise the awareness among all members of the University community on the best practices in acquiring, using, maintaining, and securing ICT facilities and information stored on them.

The following technology domains are addressed by this Policy:

1. Computing and Storage
2. Operating Systems and Applications
3. Networking and Telecommunications
4. Data and Databases
5. Security
6. Privacy
7. Systems Management and Continuity

While this Policy sets the framework for all the above domains, additional policies are to be developed as and when applicable to cover the specific aspects of each domain. A set of such policies that was agreed to be developed at the time of approval of this Policy is listed under Section 9.

3.0 Computing and Storage

Decisions on which computing hardware and storage environments to acquire, build, operate, and support are primarily based on strategic direction, the needs of existing and planned applications, staff expertise, industry trends, and efficient use of resources. Open standards, vendor neutrality, and interoperability between discrete technology components are given priority in selecting technologies to meet the University needs. Access to all forms of University owned devices and services should be provided through a proper authentication mechanism as outlined in the User Accounts and Password Policy.

3.1 Desktops, Laptops, All-in-Ones, and Workstations

Hardware selection for end-user computing is based on the specific needs of users and applications. Faculty and researchers often have different desktop computing needs than typical users. Each type of end-user computing device is broadly classified as Standard, Mid-Range, and High-End based on the application demands. Term *High-End* refers to the highest performing and most expensive of a range of computers, while *Standard* is the other end of the spectrum. The models in between are referred to as *Mid-Range*. Standard devices are recommended for a broad range of day-to-day use such as the use of productivity software, e-mail and messaging, and web access. Mid-Range computers are mostly recommended for labs to run applications such as engineering tools and simulators, software development, and desktop publishing. High-End models are recommended for specialized applications and heavy users that may need enhanced computing power, memory, storage, and/or specialized hardware. Based on this classification and commonly available models in the market, standard specifications are developed annually for each model. These specifications are based on x86, 64-bit hardware and target Microsoft Windows and Linux operating systems. macOS-compatible devices could also be purchased to run specialized teaching and research tools in classrooms and labs. The planned lifecycle for the desktop, all-in-one, and workstation computers will be 5-years and for a laptop it will be 3-years. All desktops,

laptops, all-in-ones, and workstations must be purchased with a minimum of a 3-year next day on-site warranty. For any deviations from the standard specifications, where academic, research, and/or administrative reasons warrant the purchase of a nonstandard system, special approval needs to be sought from the Director, CITeS.

3.2 Smart Computing Devices

The University recognizes the need to support smart computing devices in the classroom, labs, research, specialized projects, and other activities both within and outside the University. However, the smart computing domain is rapidly transforming making it difficult to standardize. Therefore, tablets, smartphones, and other specialized computing devices may be acquired for specialized teaching, research, and administrative duties, given that their needs are adequately justified, and a best effort is taken to comply with open standards, vendor neutrality, and interoperability with existing systems and tools. The planned lifecycle for tablets and smartphones will be 2-years and for other devices it will be 1-year. All tablets and smartphones must be purchased with a minimum of a 1-year warranty. Relevant approvals should be sought from the Director, CITeS.

3.3. Servers

Hardware selection for central computing is based on the specific needs of applications. Servers may host specialized applications for teaching, research, and administrative support; web-based services; databases; e-mail, messaging, and voice communication; internal file sharing; and other important functions of the University. UoM will utilize x86, 64-bit server hardware compatible with Linux and Microsoft Windows operating systems. All servers must be purchased with a minimum of a 3-year next day on-site warranty. Critical and sensitive servers that require high-availability shall also be purchased with a 3-year support agreement with 24x7, 6-hour response time. Blade servers are recommended due to space saving, modularity, and power saving. It is further recommended that servers support RAID 6, dual power supplies, and have an out-of-band management interface. The planned lifecycle for server hardware will be 5-years. Departments and divisions could request to utilize the central computing and data storage facility provided by the CITeS for general purpose use (e.g., storage of staff files and student projects). Procurement of server resources for general use is allowed only for special projects and special departmental server facilities. For all new hardware purchases that may need deviations from these, special approval needs to be sought from the Director, CITeS highlighting the academic, research, and/or administrative reasons.

Application performance will be reviewed after three years to determine if the server should be replaced at the end of four or five years. It is recommended that all servers are placed in the CITeS datacenter, as it provides better network connectivity, physical and network security, UPS and generator power, and climate control.

3.4 Printers, Scanners, and All-in-Ones

Selection of printers and scanners is based on the specific needs of users, applications, and printing/scanning volume. Printers are broadly classified as Desktop, Departmental, and High-Volume and include both Inkjet and Laser printers. Desktop printers are low-

end printers that are relatively slow (15 - 20 pages a minute), support printing low volume of A4 size papers, and may support full-duplex printing. Desktop printers that also support scanning and duplication are referred to as all-in-one or multi-purpose printers. While Desktop printers are relatively cheaper, cost per print is relatively high. Therefore, Desktop printers are not recommended except for special applications. Departmental printers are mid-range, multi-functional printers that print 50 - 60 pages a minute. They support printing moderate volume of full-duplex A4/A3 size papers and shared printing where multiple users could use the same printer over a wired or wireless network. While the initial cost of these printers is relatively high, cost per user is low due to sharing and the cost per print is moderate. High-Volume printers are used for bulk printing such as handouts and exam papers; hence, recommended for specialized applications only. While the initial cost of these printers is much higher, they have the lowest cost per print. Color Inkjet and Laser printers should be purchased only when required for specialized applications and use. All printers purchased must support full-duplex printing, and their default configuration should be set to automated full-duplex printing. Unless absolutely required, all printouts should be full-duplex. Use of printed materials should be minimized by utilizing emails and DMS for document sharing, meetings, student handouts and other communications as much as possible. Purchasing of additional printers are discouraged and unless absolutely necessary the Heads of the Departments should not recommend purchasing of additional printers for the division.

Scanners are broadly classified as Desktop and Document scanners. Desktop scanners are usually flatbed scanners where the paper is fed manually and supports A4 size papers (specialized engineering and architectural applications may use A3-size paper). While scanning speed is relatively low these scanners are much cheaper; hence, recommended for general use. Document scanners are designed for bulk, high-speed, full-duplex scanning of documents and can usually be shared over a network. They may also support additional features such as OCR, image enhancement, and barcode recognition. Document scanners are recommended for specialized applications only, as Departmental and High-Volume printers usually include document scanning features.

The planned lifecycle for Desktop printers will be 3-years and for other printers, it will be 5-years. The lifecycle for Desktop scanners will be 3-years and Document scanners will be 5-years. All Desktop printers and Desktop scanners must be purchased with a minimum of a 1-year warranty. Departmental and High-Volume printers, as well as Document scanners must be covered by a 3-year next day on-site warranty. All printer and scanner procurements should consider the cost and the yield of toner/ink, drum, developer, and roller, and the final decision should be made based on the Total Cost of Ownership (TCO) for an estimated print volume over 3-years. When the TCO of multiple offers is comparable, preference should be given to toner/ink cartridges that are already procured by the University for other printers to benefit from volume discounts.

4.0 Operating Systems and Applications

The operating systems and end-user applications are acquired and managed with an emphasis on perceived value, future needs, and cost containment. The portfolio of applications supported by the University can be broadly classified as:

1. Teaching and Research Applications – support the teaching and research needs of faculty and students. These applications usually include simulation/emulation tools,

development tools, mathematics and statistics tools, design and analytics tools, media editing tools, and specialized tools used with laboratory equipment. Depending on the application and license these may be installed on end-user devices, computers in labs, and servers. Teaching and research applications at the University-level include development tools, databases, and project management tools.

2. Desktop Applications – support the individual needs of faculty, staff, and students and usually include productivity software, desktop publishing, e-mail and messaging, and web access. Decisions about such are distributed across departments and divisions. Desktop applications at the University-level include productivity, mail client, and Internet browser software.
3. Enterprise Applications – support the mission-critical operations and include systems for managing student information, learning and collaboration, and exams; administrative, human resource, and financial processes; e-mail and other messaging services; and web applications. Decisions regarding such applications are centralized and priority will be given to deploying integrated technologies that are mature, stable, secure, and proven in the field.

The selection, development, and deployment of all three types of applications are often guided by the requirements, standards, and recommendations such as those imposed by:

- Professional associations and accreditation bodies
- Industry standard tools that are expected to be familiarized by students and faculty
- Widely accepted higher education practices
- Compatibility with existing hardware and operating systems
- University's ICT strategic plans
- University procurement policies and standards
- Security compliances such as Open Web Application Security Project (OWASP)
- Accessibility Standards such as W3C Guidelines
- Availability of funds and special grants

Access to all forms of operating systems and applications should be provided through a proper authentication mechanism as outlined in the User Accounts and Password Policy, as well as per the license agreements. Where applicable academic, research, and government licenses should be selected over enterprise licenses (in the order specified) for both the operating systems and applications. Applications purchased under only the academic licenses should not be used for research or consultancies, while applications purchased under only the research licenses should not be used for consultancies. Where applicable, licenses should be purchased or renewed through volume license agreements rather than via OEM (Original Equipment Manufacturer) licenses from vendors to enable easier upgrades, transitions to other devices and virtualized environments, and cost savings. Users proposing to procure operating systems and applications must ensure that requirements are well understood (including workloads, performance, and utilization requirements) and are clear of any hardware, networking, storage, and license dependencies and limitations. Relevant approvals and clarifications should be sought from the Director, CITeS.

5.0 Networking and Telecommunications

University network is designed as a collection of local networks with secure zones implemented where needed, and open segments available to foster innovation and support the needs of students, faculty, and researchers. Given the high reliance on the Internet and related technologies, as well as the requirement to interoperate with the rest of the community, the University network follows the Internet standards as implemented by the higher education communities such as the LEARN. The essential standards include standards defined by the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE) networking standards.

5.1 Cabling

Horizontal station wiring to interconnect desktops, servers, networking equipment, IP phones, and IP cameras are based on Category 6 UTP (Unshielded Twisted Pair). Other forms of network wiring to interconnect specialized devices should also utilize Category 6 UTP whenever possible to maintain the interoperability and to utilize existing wiring. RJ45 modular plugs must be wired based on the T568B Wiring Standard. University buildings will be interconnected using fiber optic cabling to gain better bandwidth, quality of service, and surge protection. Where pathways permit, each building should be connected via a separate fiber to the network distribution switches at the CITeS. All new fiber installations will make use of single-mode fiber optic cables. Two or four UTP cables or fiber optic cables should be laid when connecting mission-critical networking devices to the core network and within the server rooms. All major network wiring projects within a building, network wiring across floors of a building, and network wiring between buildings need to be approved by the Director, CITeS to ensure interoperability, optimum use of core network, and compliance with cabling and safety standards.

5.2 Networking Hardware

Network hardware includes switches, routers, wireless access points, wireless controllers, firewalls, and other network appliances. Network hardware should be powered via a UPS with at least 15-min backup power. Moreover, they should either include redundant power supplies or the capability to add a redundant power module when required (if the chassis does not support having a redundant power supply). Power over Ethernet (PoE) capabilities based on IEEE 802.3at-2009 standard (or better) are recommended over separately powered devices to ensure flexibility for current and future devices. All network hardware should be placed on a floor or wall-mounted lockable rack with adequate ventilation. CITeS staff should have physical access on a 24x7 basis to ensure proper functioning and configuration of all networking devices attached to the University network. Protocol for such access must be discussed and agreed a priory with the respective head of the department, division, or project to ensure safety, security, and privacy of equipment, data, and users. All networking hardware should support remote management, comply with IPv6 and SNMP, and must have a minimum of 3-year warranty. During each acquisition cycle, network hardware should be reviewed by validating performance and security, and replacement decisions should be made based on the importance of the device, cost, and funds availability. Relevant approvals should be sought from the Director, CITeS before procurement to ensure interoperability, optimum performance, and compliance with networking and security standards.

5.3 Internet Connectivity

Access to the Internet is provided to all faculty, students, staff, and approved project personnel as per the policies defined under the “Acceptable Use Policy” and “Information Security Policy”. In general, all users should not use social media and visit recreational websites during the working hours, as well as misuse university network resources.

Email Fcaility

University of Moratuwa shall maintain at least two high-speed connections to the Internet. These connections should use paths that are as diverse as possible to avoid a single point of failure that is likely to impact both the paths. BGP routing should be utilized for all traffic using these connections to provide automatic failover in the event of an outage on one of the connections. UoM shall leverage contracts from LEARN to maintain adequate bandwidth at cost-effective rates. Connectivity to the ITUM and any other campuses in the future should be via an IP VPN connection.

5.4 IP Addresses and Domain Names

Address assignment for the networks and devices is based on the IPv4 standard. However, as the IPv4 address space is scarce and difficult to scale, the University plans to fully comply with IPv6 by 2022. Therefore, procurement of all future network hardware should be IPv6 compliant. Departmental-level private IP ranges are assigned by the CITeS, and departments may allocate them to internal devices. However, it is recommended that the last usable address of a given IP range is used as the gateway address while the first usable address is kept unused to support future use cases unless already assigned to a specific device. All public IP addresses are assigned by the CITeS and should be leased only to the essential devices and applications that need directly reachability from the Internet. All other devices should use local IPs.

All domain names under **uom.lk** are assigned and managed by the CITeS. Relevant approvals should be sought from the Director, CITeS to use public IPs and domain names while explicitly mentioning the type of service(s) to be used and ports to be opened. Only the approved public IPs and ports will be opened through the firewall, and all other public IPs will remain blocked.

6.0 Data and Databases

Lots of data ranging from student assignments and reports, lecture notes, research papers, and research data to architectural/engineering drawings and chemical/material compositions include some form of intellectual property. Moreover, exam marks, email content, and accounting and HR data need to be protected due to the monetary value and privacy concerns. All internally communicated information, including e-mails, document management system, and other documents should be considered as the University property. Hence, should not be forwarded to outside parties without the permission of the authorized personnel as per the confidentiality level of the e-mail/document. The use and protection of University data are described in “Information Security Policy” and “Privacy Policy”. These policies identify the shared responsibilities for collecting, storing, destroying, and assuring data integrity, as well as established uniform data management standards.

The University supports databases for applications ranging from online learning, student management, library catalogue, accounting and HR, to research databases. Existing database solutions (e.g., those already used and supported by the UoM) are preferred over different but equivalent technology. Relational databases and the SQL are well-understood and have a long history of successful implementation in a variety of academic, research, and administrative applications; hence, are preferred over other alternatives such as No-SQL databases. Moreover, both the databases and database access standards should not be proprietary to avoid database vendor lock-in. MySQL Community Edition is supported and maintained by the CITeS. Other priority solutions such as Microsoft SQL Server, MySQL Commercial editions, and Oracle are recommended in the given order, for special projects and applications given a detailed justification for the use of those services and approved by the Director, CITeS, as well as relevant funds are available. No database should be operated without the licenses based on applicable use. Other forms of open source databases (both relational and No-SQL) may be used for teaching and research; however, those are not centrally supported by the CITeS.

7.0 Security and Privacy

While the Universities generally try to be open on the use of ICT facilities to foster innovation and support the needs of faculty, students, and researchers, the openness itself could make the University an easy target for attackers. Thus, ICT security and privacy are serious issues that cannot be ignored by any member of the University community who uses a computer. Even if users believe they do not have anything worth protecting on their computers, it is still important to keep it safe both from internal and external attackers, as it could lead to loss of data, loss of productivity, utilization of bandwidth, spamming, and could be the basis for future attacks on the same or different systems. Therefore, UoM aims to protect its information systems and the information stored on them that might have an adverse impact on its operations, infrastructure, or reputation if compromised. UoM ICT security program includes policy, user awareness and training, strong technical controls on computers, network systems, associated data, and data transmission. Mechanisms for the proper protection of ICT resources and their associated data are specified in the “Information Security Policy” and “Privacy Policy”.

8.0 Systems Management and Continuity

The goal of systems management is the holistic management of the ICT environment to ensure continuity of the ICT resources and the access to those resources. Systems management concerns the monitoring of ICT resources and networks for faults, performance, and intrusions; accounting for the use of resources; configuration management; and the detection and enforcement of activities that conflict with the ICT security policy. System management and monitoring activities include, but are not limited to, network monitoring, monitoring servers and applications, network and proxy traffic analysis, virtualization and storage management, wireless LAN management, event management, performance management, asset management, event and access log monitoring, and troubleshooting tools. Guidelines on systems management are largely derived from standards such as ITIL and FCAPS. “ICT Operations Policy” covers the systems management aspects while additional aspects related to continuity of ICT resources are covered in the “Business Continuity Plan.”

9.0 Supplementary Policies and Laws

This Policy is supplemented by the following policies:

1. Acceptable Use Policy
2. User Accounts and Password Policy
3. e-Mail, Web, and Social Media Policy
4. Information Security Policy (in preparation)
5. Privacy Policy (in preparation)
6. ICT Operations Policy (in preparation)
7. Business Continuity Plan (in preparation)
8. ICT Procurement Policy (in preparation)

While this Policy provides the baseline, all policies work and enforced together. Hence, a specific case should be interpreted based on the combination of this Policy and all other applicable and approved policies. University community also needs to be aware of conduct which may breach national laws and lead to civil or criminal legal proceedings and penalties for which they will be held personally responsible. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017
4. Intellectual Property Act No. 36 of 2003 of Sri Lanka

Moreover, any contracts and agreements with third parties should include means for redress by the University in the event of a dispute.

10.0 Enforcement

The UoM reserves the right to withdraw the permission granted to any user or administrator for the use of UoM ICT facilities under the following circumstances:

1. The user violating any provisions in this and subsequent policies
2. The use of ICT facilities by the user places those facilities at risk
3. The use of ICT facilities by the user poses a security or other threat to other users of the University community, the UoM, general public, or to national security
4. The user violating the privacy and personal rights of others

Additionally, the UoM may take appropriate disciplinary, administrative, and legal action under the relevant rules and regulations against the ICT policy violators.

11.0 Approval and Review

The authority to interpret this policy and subsequent policies listed under Section 9 rests with the Vice-Chancellor of the University and the University Council, and is generally delegated to the Director, CITeS. *This "Information Technology Policy" was initially approved by the University of Moratuwa Council on xxxx x, 2020. In University of Moratuwa Council minutes xxxx Dated xxxxxx, 2020,* the Vice Chancellor and Director, CITeS were granted full

continuation of the authority and responsibility for the management of the IT facilities and functions for the University.

This Policy and subsequent policies are to be reviewed annually. The Director, CITeS will ensure that reviews of this Policy, subsequent policies listed in Section 9, and subsequent revisions are performed when necessary, and will request review by the Information Technology Advisory Committee (ITAC) and the Legal and Documentation division. After review, any amendments to this Policy and subsequent policies or new policies must be approved by the University Council prior to the enforcement.

12.0 Contact Information

Users requiring clarifications and feedback with regard to this Policy, subsequent policies, or those who wish to report a breach of this Policy should contact:

Director – Center for Information Technology Services (CITeS)
e-Mail: cites@uom.lk
Phone: 4400

Abbreviations

CITeS	Center for Information Technology Services
FCAPS	Fault, Configuration, Accounting, Performance, and Security
HR	Human Resources
ICT	Information Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
ITAC	Information Technology Advisory Committee
ITIL	Information Technology Infrastructure Library
ITUM	Institute of Technology, University of Moratuwa
LEARN	Lanka Education and Research Network
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PoE	Power over Ethernet
RAID	Redundant Array of Independent Disks
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TCO	Total Cost of Ownership
UoM	University of Moratuwa
UTP	Unshielded Twisted Pair
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network
W3C	World Wide Web Consortium

Annex I

Acceptable Use Policy (AUP) for Information and Communication Technology Facilities of University of Moratuwa

1.0 Objectives

The Information Communication Technology (ICT) facilities of the University of Moratuwa (UoM) are provided to following users:

1. Internal students with a currently valid registration, either full-time or part-time
2. Staff in current employment with the UoM, either permanent or contract
3. Personnel of the UoM departments, divisions, projects, etc., with a valid authorization for the use of ICT facilities given by the Head of the relevant unit
4. External users with a currently valid authorization for ICT facilities use either by the Head of the relevant department/division or Center for ICT Services (CITeS)

Above users are given access to the UoM ICT facilities for the purpose of:

1. Conducting and participating in academic coursework and research
2. Performing and using academic and non-academic administrative services
3. Conducting and participating in University-approved student and staff welfare services
4. Conducting and participating in University-approved projects

For reasonable use, the students and staff are not charged a fee, and the UoM bears the cost of providing access to the UoM computing, storage, and network (including Internet) resources. The objective of this Acceptable Use Policy (AUP) for ICT facilities of the UoM is to protect the essential interests of the UoM without unduly restricting the use of ICT facilities and services which have been established for the greater benefit of the students, staff and the UoM generally.

2.0 ICT Facilities Covered Under AUP

For the interpretation and application of this AUP, a *computer* is defined as a digital device that can store and process data with interfaces for external communication and data transfer to and from other devices or communication networks. Smart devices such as phones, tablets, and wearables are considered as computers under this definition.

This AUP is applicable to the following equipment and services:

1. To all computers (University owned or otherwise) while they are located inside the UoM premises including campuses, project building, and hostels
2. To all computers, computer peripherals, detachable storage devices, and network equipment (University owned or otherwise) while they are connected to the UoM wired and wireless networks
3. To all University-owned computers, computer peripherals, services, and software that are used outside the UoM premises

4. To all ICT equipment provided in lecture theaters, laboratories, and offices
5. To all Internet accesses, remote access, and electronic messaging services (e.g., e-mail, IM, VoIP, chat sessions, IRC, and newsgroups) using UoM ICT facilities
6. To all user accounts provided on UoM ICT systems
7. To all types of data stored on UoM ICT systems
8. To all proprietary and open source software for which the UoM hold licenses and to the software developed by the UoM

3.0 Permitted Activities

The UoM ICT facilities are expected to be used for the following activities in general:

1. Access to authorized academic course materials, research resources, and online activities hosted within the UoM ICT facilities
2. Access to materials hosted outside the UoM ICT facilities for study, research, and academic or non-academic administrative purposes
3. Access to software and equipment used in an academic study, research, and academic or non-academic administrative work hosted within the UoM ICT facilities
4. Access to software and equipment hosted outside the UoM ICT facilities for study, research, and academic or non-academic administrative purposes
5. For organizing and managing academic, research, and administrative work
6. For organizing and managing University authorized, extra-curricular activities
7. For the development of software for academic, research, and administrative purposes
8. For limited recreational purposes that are in strict conformity with this AUP including restrictions on resource usage, time of use, intellectual property rights, applicable civil and criminal laws. The recreational activities shall be strictly limited to listening to music, viewing videos, and participating in messaging, social networking, and media sites. Such recreational activities should not be offensive, disturbing, or embarrassing to any member of the UoM community or outside.

4.0 Prohibited Activities

The users of UoM ICT facilities are strictly prohibited from misusing those equipment, services, and facilities. Following are some examples of prohibited activities

1. Unauthorized access to user accounts – Users are expressly prohibited from accessing UoM ICT facilities from an account other than their own
2. Unauthorized access to ICT resources – Users are expressly prohibited from unauthorized access to any equipment, data, and services on UoM ICT facilities
3. Unauthorized installation of programs – Users are strictly prohibited from installing unauthorized programs (proprietary or open source) on UoM ICT facilities
4. Conduct of unauthorized commercial activities – Users are not permitted to run a for-profit or non-profit business on UoM ICT facilities without authorization from the relevant UoM authorities
5. Examinations, Assessments, and Assignments – Users are not permitted to use ICT facilities to sell, purchase, or broker in assignments, to solicit or offer to write assignments for others
6. Unauthorized electronic messaging – Users are strictly prohibited from using electronic messaging services form knowingly originating or retransmitting messages that are defamatory; aggressive or rude to other users; threatening or harassing; containing political and religious views, containing sexually explicit content; bulk, unsolicited, and

spamming; chain e-mail; seeking to impersonate another person (spoofing); containing malware such as viruses, worms, and Trojans

7. Unauthorized access to third-party resources – Users are strictly prohibited from using UoM ICT facilities to access any third-party (within or outside the UoM) user accounts, material, data, services, and equipment that they do not have the authorization to access
8. Unauthorized access and dissemination of information – Users are strictly prohibited from unauthorized access, dissemination, and storing of sensitive information such as intellectual property, proprietary material, course notes and material, agreements in the form of MoUs and NDAs, internal memos, and data
9. Plagiarism – Users are strictly prohibited from engaging in plagiarism
10. Game playing – Game playing is not allowed on UoM ICT facilities without authorization
11. Peer-to-peer services – Users are strictly prohibited from using peer-to-peer services to access or share copyrighted material, enable anonymous access to third-parties via proxy and VPN (Virtual Private Network) services, cryptocurrencies, etc.
12. Pornography – Users are strictly prohibited from accessing pornographic materials using UoM ICT facilities. The creation, storage, or distribution of pornographic materials is also strictly prohibited
13. Unfair use – Users are strictly prohibited from using UoM ICT facilities in a manner that is inequitable or disruptive to other users

5.0 Responsibilities of Users

All the users of the UoM ICT facilities must cooperate with other users, systems administrators, and the UoM authorities to ensure fair and equitable access to the resources by all. Users of the ICT facilities must be aware of the conditions on which the access is provided, as well as permitted and prohibited activities.

Access to the UoM ICT facilities is provided through a computer account identified by a username and protected by a password. Therefore, it is strictly required that:

1. Users must not divulge their passwords to anyone
2. Users must not knowingly engage in any activity to obtain the passwords of other users
3. Users must access UoM ICT facilities using only their own computer usernames
4. A user must immediately change his or her password and inform the relevant systems administrator if a password compromise is suspected
5. Users must follow the guidelines provided by the relevant systems administrators and University User Accounts and Password policy in selecting and keeping a secure password and logging-off after use of ICT services

In determining the fair and reasonable use of UoM ICT facilities, users should use their discretion. The UoM from time to time will inform the users on specific limits on the usage and quotas made available. Users are expected to adhere to these limits, and the UoM reserves the right to levy charges it deems appropriate for usage above-set limits.

The UoM accepts no responsibility for:

1. Direct or consequential losses or damages due to the use of the UoM ICT facilities for academic, non-academic, or personal purposes
2. Loss of data or interference with files and services due to the UoM's efforts to maintain, protect, and improve the ICT facilities

Unlawful use of ICT facilities by a user will breach this AUP and will be dealt with as a disciplinary offense. Unlawful use of ICT facilities may lead to civil and criminal legal action being taken against individual users. The UoM will not defend or support any user who uses UoM ICT facilities for unlawful purposes.

6.0 Privacy and Surveillance

The UoM reserves the right to access, inspect, and monitor e-mail, websites (official and personal), server and firewall logs, electronic files and data, software, computers, or any electronic device that is:

1. Connected to the UoM network, both wired and wireless
2. Operated inside the UoM premises either permanently or temporarily, irrespective of the ownership of the equipment

Following high-level, UoM-wide monitoring is in place on a 24x7 basis:

1. Firewall logs for initiating and accepting network connections, as well as attempts to access/use blocked services and ports
2. Proxy logs for initiating connections to URLs
3. Wireless access log
4. Applications logs such as e-mail, Moodle, and LearnOrg
5. Server logs

The UoM will conduct these inspection and monitoring activities if it determines that there is a reason to do so. Such reasons include, but are not limited to:

1. Suspected or reported breaches of this AUP
2. Suspected or reported breaches of any rules, regulations, or policies of the UoM
3. Suspected or reported breaches of the Law

7.0 Relevant Laws

Users need to be aware of conduct which may breach national laws and lead to civil or criminal legal proceedings and penalties for which they will be held personally responsible. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017
4. Intellectual Property Act No. 36 of 2003 of Sri Lanka

8.0 Measures on AUP Violations

The UoM reserves the right to withdraw the permission granted to any user for the use of UoM ICT facilities under following circumstances:

1. The user violating any provisions in this AUP
2. The use of ICT facilities by the user places those facilities at risk
3. The use of ICT facilities by the user poses a security or other threat to other users, the UoM, general public or to national security
4. The user violating privacy and personal rights of others

Additionally, the UoM may take appropriate disciplinary, administrative, and legal action under the relevant rules and regulations against the AUP violators.

9. Contact Information

Users requiring clarifications and feedback with regard to this AUP or those who wish to report a breach of this AUP should contact:

Director – Center for Information Technology Services (CITeS)
e-Mail: cites@uom.lk
Phone: 4400

Annex II

University of Moratuwa
e-Mail, Web, and Social Media Policy

1.0 Objectives

Internet and e-mail services are vital for the University of Moratuwa (UoM) to function as a modern higher learning and research institution, and to further its vision and mission. However, these resources could be misused, either accidentally or intentionally, without a governing framework on the acceptable use of the resources. Social media provides unique and rich opportunities to converse with the University community and beyond, as well as share information enhancing the image of the University and its stakeholders. However, improper use could pose risks to the University's reputation, confidential and proprietary information, and compliance with laws and regulations. To minimize these risks, the objective of this Policy is to protect the essential interests of the UoM without unduly restricting the use of e-mail, web, and social media facilities and services which have been established for the greater benefit of the students, staff, and the UoM generally.

2.0 Scope

This Policy provides guidelines for the management and usage of electronic mail (e-mail), all web-based activities, and social media. For the interpretation of this Policy e-mail, web, and social media are defined as follows:

1. e-mail – Is the electronic transfer of information, typically in the form of electronic messages, memoranda, and attached documents, from a sending party to one or more receiving parties.
2. Web – Aka., World Wide Web (WWW), is a subset of the Internet consisting of the pages that can be accessed by a Web browser. These specially formatted pages support links to other pages, as well as graphics, audio, and video files.
3. Social Media – Are the tools and online spaces for integrating and sharing user-generated content to engage in conversation and to participate in content and community creation. Example social media platforms include, but are not limited to, Facebook, Twitter, LinkedIn, YouTube, podcasts, WiKis, forums, and blogs.

Following definitions are associated with the use of those services:

1. Account holder – Is a student, faculty, staff, and other individual affiliated with the University who have been assigned an e-mail account that provides access to the University's e-mail systems.
2. Compromised account – An account that has been maliciously broken into and could be used by an unauthorized individual for nefarious reasons.

3. Content Management System (CMS) – Software, or a suite of software applications, that is used to prepare, publish, and manage content in a web-based format.
4. Illegal activities – Include, but are not limited to, obscenity; pornography; threats and harassment; theft, unauthorized access and disclosure of data; attempting to intercept any electronic transmission without proper authority; and violation of copyright or defamation law.
5. Mailbox – Is the destination to which e-mail messages are delivered. It is the equivalent of a letterbox in the postal system. It also stores the messages sent by the user.
6. Official University Communication – Includes communication that relates to work for or study with the University, including its functions, goals, or business. For example, communication with students; among faculty, staff, and administration on academic, research, and administrative matters; alumni; government; external parties such as research collaborators, professional bodies, and University business partners.
7. Personal/External e-mail Account – Any e-mail account not created and issued by the CITeS, departments, or divisions.
8. Sensitive Data – Data that is subject to national restrictions governing its processing, storage, transmission or use, or that could cause significant harm to the University or its constituents if disclosed. Examples include Personally Identifiable Information (PII), credit card information, and research data.
9. University-Wide Communication – Refers to communication with all or a large sub-group of users such as all staff, all faculty, and a batch of students.
10. University Web Presence – All web pages available on the Internet which purport to represent all or part of the UOM, including web pages associated with the content, applications, blogs, social media, and other web-based services.
11. University Websites – A subset of the University's web presence, encompassing all web pages either hosted under the *uom.lk* domains, sub-domains, or hosted on the University servers.
12. Web Administrator – The person who installs and maintain the hardware and software infrastructure hosting the website(s), as well as monitor website traffic.
13. Web Content Creator – The person who creates written, photographic, audio, video, and all other materials for websites or social media.
14. Web Developer – The person who designs and programs websites.

This Policy applies to all students, faculty, staff, consultants, temporary employees, guests, volunteers, and contractors of the University. This Policy and the guidelines apply even if a user's online and social media activity is anonymous or under a pseudonym. This Policy and the associated procedures and guidelines provide a framework for the appropriate, effective, and efficient use of UoM e-mail and Internet resources. The Policy also addresses related issues of privacy, confidentiality, security, and users' legal obligations. Moreover, this Policy should be interpreted along with the UoM's Acceptable Use Policy (AUP), user Accounts and Password Policy, Information Security Policy, and Information Communication Technology (ICT) Policy.

2.0 Electronic Mail (e-mail)

e-mail supports the educational, research, administrative, and outreach mission of the University by serving as an official form of communication for account holders within the UoM community. Access to University e-mail is a privilege with certain accompanying responsibilities. Therefore, it is essential to comply with applicable laws and University

policies; to protect sensitive University data; and to ensure the successful delivery of communications by and between the University, students, faculty, staff, alumni, government, and business partners while using e-mail.

3.1 e-mail Accounts

1. A user will be issued an e-mail account as per the User Account Creation procedure outlined in the University User Accounts and Password Policy. The format of an e-mail identifier (ID) and validity of an account are further specified in the User Accounts and Password Policy.
2. In addition to an e-mail account issued to an individual based on his/her legal name or registration number (in case of students), role-based accounts (e.g., *dean-eng*, *sar-exams*, and *info*) are also issued with the objective of unifying and archiving the communications regardless of the individual who play that role at a given time.
3. Some users may have more than one affiliation with the University. For example, a faculty member who is also an alumnus, a staff member who may be a student, and a faculty member who is a director of a center. A person with multiple roles may receive multiple accounts. In such cases, the respective account must be used for the appropriate communication. For example, a staff member who is a student should use his/her student account to engage with the research supervisor.
4. A administrative e-mails related to a user's role must originate from the role-based account. Those accounts need to be handed over to the successor when the user leaves the position.
5. Departments, divisions, and projects may have their own e-mail under sub-domains of the university subject to the prior approval of the Director, CITeS. In such cases, relevant policies need to be developed by the respective department, division, and project in line with this Policy, and those policies must be approved by the University ICT Strategy Committee within three (3) months of the launch of service. Else, the e-mail service must be terminated.

3.2 Use of e-mail

1. Account holders who are granted a University e-mail account are expected to check it regularly to receive University communications.
2. For all official University communication, all users must **only** use their *username@uom.lk* e-mail. For role-specific communication, the role-based username must be used.
3. Use of all e-mail accounts must comply with the Permitted and Prohibited Activities specified in the University Acceptable Use Policy (AUP).
4. The University highly discourages the use of e-mail to communicate research or business sensitive data. To avoid inadvertent disclosure of sensitive data, users should exercise caution when responding to or forwarding e-mail messages. As a further precaution, all potentially sensitive attachments must be encrypted and protected with a password of sufficient complexity (as outlined in User Accounts and Password Policy). The password must be securely shared off-line (i.e., through other means than e-mail).
5. All e-mail received on a personal/external account that relates to University business should be forwarded to the recipient's University-issued e-mail account. The recipient should also notify the sender to use the University e-mail for future correspondence.

However, spam and other unsolicited messages may be deleted immediately without notifying the sender.

6. Users may automatically forward e-mails received on a University-issued e-mail account to a personal e-mail account. However, e-mails received on a role-based account can be forwarded only to a University-issued personal e-mail account. When forwarding, a copy of the message must be kept in the original account regardless of whether it is a University-issued personal or role-based account.
7. The University highly discourages a user sending messages from personal e-mail account such that they appear to be from a University-issued e-mail account. Such messages are likely to be marked as spam by the recipient's e-mail system or may not be delivered at all as domain authentication is not set up for third-party mail services.
8. Each mailbox has a limited quota which varies depending on the user's role. Once the quota is reached, user will not be able to send or receive e-mail. Thus, a mailbox should be regarded as only a limited and temporary repository for e-mail. Messages and attachments should be deleted, if no longer needed, or more permanently stored on a persistent data store (e.g., hard drive or cloud backup).
    a. From time-to-time CITeS may set the following limits as per the availability of resources and the technologies advances (details will be specified at CITeS website):
        i. Size of an e-mail (including attachments) that can be sent or received.
        ii. Number of recipients that may be addressed in an e-mail.
        iii. Number of messages that can be sent per minute/hour.
        iv. Number of total messages/recipients that can be sent per 24-hour window.
        v. Messages in Junk/Spam e-mail folder may be automatically deleted after 30 days.
    b. Change of mailbox quota or exceeding the above limits is allowed only in exceptional cases and under the prior approval of the Director, CITeS.
9. While CITeS takes reasonable measures to backup the e-mails to protect against system failure; however, recovery is not guaranteed under all cases. Items removed from a user's *Deleted Items* cannot be recovered. Hence, users are recommended to backup their own mailboxes or selective messages.
10. No University-issued e-mail address can be used to create a profile on social media or other online tools utilized for personal use.

3.3 e-mail Lists

e-mail is a strategic tool for carrying out the University's mission where it can be used to communicate with large groups of people effectively. Recognizing this need, regularly replenished bulk, e-mail groups are established to enable high-level offices, departments, and divisions to reach large segments of the University community.

1. Generally, official messages come from the administration or its representatives, to be sent to the entire University community or large subgroups. Therefore, University-wide communication that has been authorized as an official communication should be received and read as any other official document at the UoM, as they may affect day-to-day activities and responsibilities.
2. University-wide communication is restricted to those e-mails that meet one or more of the following tests:

a. The message is essential to the proper execution of the daily business of the recipient group(s).
b. It notifies the recipient group(s) of significant events or changes in governance, policy, and practice.
c. It alerts the community on situations around health and safety, e.g., crime alerts.
d. It keeps segments of the recipient group(s) informed of their business. For example, an instructor sending an e-mail to the students about course-related matter, and a convener of a committee sending messages with minutes, updates, and announcements.
e. Messages that do not meet these requirements of urgency and/or critical information are blocked; hence, should seek other methods of relaying their information. Messages may also be automatically blocked when certain words in the message are identified as potential spam.

3. The membership list of a particular group belongs to the offices/roles which maintain them. As such, these e-mail list owners have the right to communicate with their constituents as they deem best, without the need for further authorization. These offices/roles may delegate to other offices or individuals the authority to communicate with these groups. However, it is expected that this delegation will parallel the existing delegation models of paper-based communication.
4. To create a new mailing list, relevant details and justification should be sent to the Director, CITeS for approval. A request will not be honored, if it does not meet the requirements specified in Item 3.3.2 above. Once approved, e-mail list will be created and authorized user(s) who could send messages are pre-assigned. CITeS will maintain University-wide e-mail lists while delegating authorized users to send messages to the respective group.

3.4 Privacy and Surveillance

1. e-mail transmission over the Internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users should use caution when assessing the authenticity, integrity, and confidentiality of any message that is sent or received via the Internet. While accessing:
    a. Web-based e-mail must be accessed via HTTPS
    b. E-mail clients and forwarding must always use secure connections (SSL/TLS)
2. The contents of all University-issued e-mail accounts are the property of the University, not the account holder.
3. As specified in the AUP, the University reserves the right to monitor e-mail to ensure compliance with applicable laws and University policies. The University also reserves the right to access and review all electronic information transmitted over or stored in e-mail and to release to third-parties when required.
4. An e-mail which is created or received by a University e-mail account in connection with the transaction of official business of the University is considered a public record, and is subject to inspection and copying in accordance with the national law.
    a. While e-mails created or received for personal use, are not generally considered public records and do not fall within the definition of public records by virtue of their placement on a government-owned computer system. However, if the University identifies any misuse of the e-mail system, personal

e-mails that are identified as being in violation of the University policy may become public record as part of an investigation.

b. A compromised University e-mail account will be promptly remedied through appropriate actions outlined in the Information Security Policy. Accounts that exhibit a repeated pattern of compromise will be suspended until the completion of an inquiry. Where applicable, the account holder may have to complete appropriate training.

3.0 Web Access and Publishing

CITeS provides web hosting services to all University entities. The use of websites must be in support of educational, research, and professional activities that are consistent with the educational goals and policies of the University. This section of the Policy applies to all forms of University web presence, whether created by the University, departments, staff, or students.

3.1 University Websites

1. The university website *.uom.lk is the sole property of UoM. University also owns the *.*uom.lk* domain. Unless for specialized and approved applications, University web presence must only be on *.*uom.lk*. While certain staff will have access to edit certain portions of the website, create new content, and remove old content, the website and all its sub-sites remain the property of the University.
2. University websites will convey the UOM brand and reflect the University's broad values and culture. As it will be clearly identifiable as a part of the University, a consistent and identifiable representation of the University is of utmost priority.
3. The University website is the responsibility of the Director, CITeS (or their nominee).
4. Only the content provider (i.e., respective Head/Director of the department/division) may request from the Director, CITeS to set up a UoM organizational unit website for the department, division, or project. Any requests for a new website should include the following:
    a. The contact details of the content owner and website developers/moderators
    b. The high-level structure of the website and what content will be presented on the website
    c. The visual design of the website (if different from the visual designs available through the University Content Management System (CMS))
    d. Any special technical requirements for the site (databases, wikis, web services, and APIs).
    e. Anticipated workload such as types and sizes of content, users and their access patterns
5. Once the request is approved, a separate username and password pair must be issued for the development and maintenance purposes of the website. Moreover, if other resources such as database access is needed, a separate account needs to be issued for each service. All such accounts should be created in-line with the User Accounts and Password Policy.
6. The establishment and maintenance of such a department, division, or project website may be delegated with the permission from the respective Head/Director to named individuals within the department/division.
7. All websites of departments, divisions, or University projects must be under the *uom.lk* domain. In special circumstances, departments, divisions, and projects may have other

domains given strong justification and prior approval of the Director, CITeS. In such cases, relevant policies need to be developed by the respective department, division, and project in-line with this Policy, and those policies must be approved by the University ICT Strategy Committee within three (3) months of the launch of the website. Else, the website must be terminated.

8. To ensure consistent maintenance and application of patches and security updates all University websites must be hosted on the CITeS-managed web servers.

3.2 Web-based Content Access, Creation, and Hosting

1. Accessing, creating, hosting, and sharing content related to the University's web presence, as well as using the University ICT resources must comply with the Permitted and Prohibited Activities specified in the University Acceptable Use Policy (AUP).
2. Any requests for changes to the University website must be made through the Director, CITeS (or their nominee) and will be reviewed on a case-by-case basis.
3. Users are encouraged at all times to use their department, division, or project websites to communicate in a responsible manner having due regard to the rights and reputation of the University and of others as outlined in the AUP.
4. CITeS Web Administrator must be consulted before a new website is created to ensure consistency, technical compatibility, and security. All efforts must be taken to implement new websites through the CMS provided by the CITeS.
5. All University websites must be responsive such that they work with popular web browsers and common screen sizes.
6. Homepages of all University websites must identify themselves as members of the University administration. Therefore, homepages of all University websites must contain a link to the University Homepage and University's Privacy statement.
7. Use of the University logo and branding on department, division, or project websites is subject to the University branding guidelines.
8. Each website must contain contact details of the department, division, or project, as well as an e-mail address that is regularly followed up by the web content creator or web developer.
9. Publications must include a statement of copyright and sharing policy when appropriate. When including copyrighted materials indicate that the permission has been received.
10. All University web pages should meet the goals of high quality in both style and presentation. All websites must be regularly updated. Correct grammar and spelling are expected.
11. Any website, web services, or REST APIs exposed (internally or externally) must be in line with the Information Security Policy.

4.0 Social Media

Social media provides unique and rich opportunities to converse with the University community and beyond. However, improper use could pose risks to the University's reputation, confidential and proprietary information, and compliance with laws and regulations. These concerns are relevant even to your personal accounts, as you will be seen as a student, faculty, staff, or affiliate of the University. Therefore, this section of the Policy applies to all forms of University and personal social media sites/presence whether created by the University, departments, staff, or students.

4.1 University Social Media Sites

1. This includes the official social media sites created by the University (including repositories of material such as WiKis and Forums for Staff and Students), as well as University profile pages created on third-party sites such as Facebook, Twitter, LinkedIn, and YouTube.
2. University social media sites will convey the UOM brand and reflect the University's broad values and culture. As it will be clearly identifiable as a part of the University, a consistent and identifiable representation of the University is of utmost priority.
3. The University social media pages are the responsibility of the Director, CITeS (or their nominee).
4. Only the content provider (i.e., respective Head/Director of the department/division) may request the Director, CITeS to set up a UoM organizational unit social media site for the department, division, or project. The request should include the following:
    a. The contact details of the content owner and content developers/moderators.
    b. The reason for having a separate account/presence that is different from the existing University social media sites.
5. Once the request is approved, a separate username and password pair must be issued for each social media site in-line with the User Accounts and Password Policy. "UoM" must be used as part of the account name while creating an account on a social media platform.
6. The establishment and maintenance of such a department, division, or project social media site may be delegated with the permission from the respective Head/Director to named individuals within the department/division.

4.2 Personal Accounts on Social Media Sites

1. While UoM does not limit the private use of social media, it is important to note that the same professional expectations; guidelines for interacting with students, alumni, media, and other university constituents; and national laws apply online as in person. As a student, faculty, and staff of the University, you represent UoM both in and outside of your classroom and office, and are responsible for anything posted on your personal social media sites.
2. Third-party social media sites, such as Facebook, Twitter, YouTube, and LinkedIn are used at the user's own risk. As the university has no control over these sites, the university cannot take any responsibility for data stored on these sites.
3. Users should familiarise themselves with the terms and conditions governing each social media site and adhere to these conditions, in addition to the regulations set out in this Policy and AUP.
4. Users should ensure that they protect themselves, read and familiarise themselves with any privacy policy governing the social media site to ensure that they accept the disclosures that may be made of their data. It is highly recommended that users maintain the highest possible privacy settings on those sites (e.g., a *private* profile on Facebook).
5. Think before you post. Even when social media accounts have been deactivated, copies of user information may still remain online. Therefore, before posting content, users should consider the permanent online footprint they are creating in doing so.

4.3 Social Media Content Access, Creation, and Sharing

1. Accessing, creating, and sharing content related to the University and personal social media sites must comply with the Permitted and Prohibited Activities as specified in the University Acceptable Use Policy (AUP).
2. Any requests for changes or to add a new post to a University's social media site must be made through the Director, CITeS (or their nominee) and will be reviewed on a case-by-case basis.
3. Users are encouraged at all times to use their department, division, or project social media sites to communicate in a responsible manner having due regard to the rights and reputation of the University and of others as outlined in the AUP.
4. All University social media sites must identify themselves as members of the University administration.
5. Use of the University logo and branding on department, division, or project social media sites is subject to the University branding guidelines.
6. Each social media site must contain contact details of the department, division, or project, as well as an e-mail address that is regularly followed up by the web content creator or web developer. Content owner (or their nominee) is responsible for monitoring and maintaining the site and should check the sites/e-mails for new posts/comments at least once a week.
7. All messages posted by followers must be moderated before appearing on any University social media site. Any posts/comments that are illegal, obscene, defamatory, harassing, discriminatory, threatening, infringing on the intellectual property rights of others, an invasion of privacy, or violation of AUP must not be published.
8. Publications must include a statement of copyright and sharing policy when appropriate. When including copyrighted materials indicate that the permission has been received.
9. All University social media pages should meet the goals of high quality in both style and presentation. All social media sites must be regularly updated with at least one post per month. While the language used can fit the style of the particular social media platform, care must be taken to preserve the semantics of the message, and not to have obvious grammar and spelling errors.
10. Unless authorized to speak on behalf of UoM as part of a user's job responsibility, users must be clear to the readers that the views expressed are yours alone and that they do not reflect the views of the University, by stating, for instance, "The views expressed in this post are my own. They do not represent the positions, strategies, or opinions of the University of Moratuwa."
11. University strongly urges that faculty, instructors, supervisors, and managers not ask to be a part of a student's or subordinate's social media network. Any student, faculty, or staff may reject, without fear of retaliation, any request from any other student or employee that, if accepted, would permit access to a private social media site or page.

5.0 Supplementary Policies and Laws

This Policy is supplemented by following policies:

1. Information Technology Policy
2. Acceptable Use Policy
3. User Accounts and Password Policy

4. Information Security Policy
5. Privacy Policy
6. ICT Operations Policy

These policies work and enforced together; hence, a specific case should be interpreted based on the combination of this Policy and all other applicable and approved policies. University community also needs to be aware of conduct which may breach national laws and lead to civil or criminal legal proceedings and penalties for which they will be held personally responsible. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017

6.0 Enforcement

The University reserves the right to monitor, intercept, and review, without notice, the postings and activities of students, faculty, staff, and other users where there is a reason to suspect that this Policy is being breached, or where deemed necessary by the University for other legitimate reasons. The CITeS will need the approval of the University Administration to access specific e-mail and data for the above-specified purposes. The extent of the access will be limited to what is reasonably necessary to acquire the necessary information.

The UoM reserves the right to withdraw the permission granted to any user or administrator to access e-mail, websites, social media, and other ICT facilities, if the user does not comply with this Policy and associated University policies as outlined in Section 5.0. Additionally, the UoM may take appropriate disciplinary, administrative, and legal action under the relevant rules and regulations against this policy violators.

7.0 Contact Information

Users requiring clarifications and feedback with regard to this Policy, subsequent policies, or those who wish to report a breach of this Policy should contact:

Director – Center for Information Technology Services (CITeS)
e-Mail: cites@uom.lk
Phone: 4400

Abbreviations

API	Application Programming Interface
AUP	Acceptable Use Policy
CITeS	Center for Information Technology Services
CMS	Content Management System
ID	Identity/Identifier
IT	Information Technology
ICT	Information Communication Technology
PII	Personally Identifiable Information
REST	Representational State Transfer
SSL	Secure Socket Layer
TLS	Transport Layer Security
UoM	University of Moratuwa
WWW	World Wide Web

Annex III

University of Moratuwa
User Accounts and Password Policy

1.0 Objectives

Generally, access to the Information Communication Technology (ICT) facilities of the University of Moratuwa (UoM) requires users to prove their identity to the respective system(s). This is usually achieved by the use of a username and password combination. This document provides a unified policy on how user accounts are to be created and requirements on the complexity, transfer, use, and storage of passwords and other authentication credentials. This policy to be applied uniformly across all of the University ICT facilities and to be interpreted along with the UoM's ICT Policy and Information Security Policy.

2.0 User Accounts

2.1 Types of Accounts

A *User* is anyone who accesses UoM ICT facilities, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, consultants, temporary employees, guests, volunteers, and contractors. More specifically:

1. Internal students with a currently valid registration, either full-time or part-time
2. Staff in current employment with the UoM, either permanent or contract
3. Personnel of the UoM departments, divisions, projects, etc., with a valid authorization for the use of ICT facilities given by the Head of the relevant unit
4. External users with a currently valid authorization for ICT facilities use either by the Head of the relevant unit or Center for IT Services (CITeS)

Access to the UoM ICT facilities is provided through a computer account identified by a username. Thus, *User Account* is a unique reference assigned to a user to enable a computer system to identify that individual uniquely. User accounts are further classified whether it is given for a faculty member, member of administrative staff, student, visitor, to reflect a specific role, task, or event, or for a project. An account not used by a user, but by one computer system connecting to another computer system, is referred to as a *System Account*. Username assigned to both user and system accounts should be unique where precisely one user or service must be mapped to an account.

2.2 User Account Creation

All authentication should take place using the University's central authentication services. When system-level constraints prevent the use of central authentication and/or full implementation of this Policy, CITeS needs to be informed of the limitation, and possible cause of actions should be discussed and agreed with the Director, CITeS before commissioning of those services or hardware equipment for production use.
A user account should be created by CITeS or other systems Administration only when a written or e-mail request is received from the respective head of the department (in case of e-mail requests, the official e-mail address should be used). User accounts for students should be created only via a request from the Examination and Registration Division. A typical request to create an account should include the following details:

1. Full name of the user, role, task, or project
2. NIC No, Student ID, employee ID, or other forms of ID as applicable for the type of account created
3. Contact details, e.g., phone no and alternative e-mail address
4. Type of account
5. User's full-time/part-time status
6. Account active duration (for visitor, event, or project accounts only)
7. Name of department or division
8. 2 to 3 preferred usernames as per the guidelines in Section 2.3

A user will be given access to a particular information system, hardware, or network only if such operation is a part of, or directly related to the teaching, learning, research, or administrative workload of the academic or administrative unit.

2.3 Format of a Username

Depending on the user's role a username should be an alphanumeric string in the format specified in Table 2.1. In all possible cases, every attempt must be taken to issue a unique username that works across all University services such as e-mail, LMS, and MIS. Usernames are given on a first come first serve basis. Alias is given only under specific circumstances, and a detailed justification for the use of the alias needs to be given.

The request must be approved by the Director, CITeS before to creating the alias. In case of an alias primary username should still be in line with the Table 2.1.

Table 2.1 - Recommended format of a username.

Account Type	Constraint	Format	Example
Faculty and administrative staff member	Must reflect part of the name	<<first name>>.<<last name>> <<first name>><<first character of last name>> <<initials>><<last name>>	saman.desilva samans abcdesilva
Undergraduate student accounts	Should reflect students ID and must reflect batch	<<last name>> <<initials>> <<batch number>> Duplicates <<last name>> <<initials>> <<duplicate number>>	udayanganihdn 13 Duplicates udayanganihdn 2.13

		.<<batch number>>	
Postgraduate student accounts	Should reflect students ID and must year of registration	<<last name>> <<initials>> <<last two digits of year of registration>> Duplicates <<last name>> <<initials>> <<duplicate number>> . <<last two digits of year of registration>>	udayanganihdn 20 Duplicates udayanganihdn 2.20
Visitor accounts including visiting lecturers and volunteers	Prefix must reflect visitor status	vl-<<first name>> vl-<<first name>>.<<last name>> vl-<<first name>><<first character of last name>> vl-<<initials>><<last name>>	vl-saman vl-saman.desilva vl-samans vl-abcdesilva
Role and task specific accounts	Must reflect role or task	<<short name of role/task>> - <<department/division>>	head-CE help-cites library
Event and project specific accounts	Must reflect event or project. Should reflect department/division	<<short name of event/project>>	exmo mercon
Systems administrator accounts	Must reflect administrator	<<admin role>>	admin mis-admin

2.4 Validity of an Account

Valid duration of an account varies based on the type of user and anticipated duration of use as listed in Table 2.2. In addition to these maximum limits, an account may be disabled at any time by a written or e-mail request from the Head of the department/division, Examinations and Registrations division, or ICT Strategy Committee. On special circumstances such as termination of a user's service, particular account should be disabled immediately. It is solely the responsibility of the user's superior to inform CITeS and other delegated administrators when such changes are necessary using required documentation. Moreover, CITeS and other delegated department/division level administrators may disable an account when the user poses a security or other threat to other users of the University community, the UoM, general public or to national security. After disabling, all accounts should still be retained for at least 3 months before terminating/deleting from the system(s). All user access will be reviewed no less than annually for critical information systems.

Table 2.2 - Validity period of an account.

Account Type	Valid Period
Faculty and administrative staff member	3-months after retirement, transfer, change of role, or resign.
Undergraduate student accounts	3 months after graduation

Postgraduate student accounts	3months after graduation
Visitor accounts including visiting lecturers	3-months for visiting lecturers and 1-month for all other visitors
Role and task specific accounts	3-months from the date the role or task becomes invalid.
Event and project specific accounts	3-months after even or end of projects. Valid period is not defined to annual events or projects.
Systems administrator accounts	System lifetime

Alternatively, an account may automatically get disabled or locked out at least for one hour, where a password for an account has been entered incorrectly at least three (3) consecutive times.

3.0 Passwords

Users' access to UoM ICT facilities is usually protected by a *password*, which is a secret string of letters, numbers, and/or symbols that is used to prove the identity/username of a user. Therefore, it is strictly required that:

1. Users must not divulge their passwords to anyone including CITeS and other administrative staff
2. Disclosed of user name and passwords to anyone by students would be a punishable offense
3. Users should not reveal passwords via e-mail and phone, as well as not cache using remember password feature of applications such as web browsers and mobile apps
4. Users who have access to multiple user accounts (depending on their role and services being accessed), should not use the same password across different University and non-University user accounts
5. Users must not knowingly engage in any activity to obtain the passwords of other users
6. Users must access UoM ICT facilities using only their usernames
7. A user must immediately change his or her password and inform the relevant systems administrator if a password compromise is suspected
8. Users must follow the guidelines provided by the relevant systems administrators and University password policy in selecting and keeping a secure password and logging-off after use of ICT services

In addition to passwords, other forms of authentication such as fingerprints, access cards and tokens (magnetic strip and NFC based ones), device signing, and digital certificates may be used for specialized applications. In such cases, due care should be used to issue, transfer, use, and store those credentials similar to that of a password. In future, two-factor authentication must be used for administration of business-critical and sensitive systems such as LMS, MIS, and accounting and HR. By 2021, two-factor authentication should be used for all access to University ICT facilities initiated from outside the campus.

3.1 Password Complexity

A password should be an alphanumeric string consists of characters, numbers, and symbols in the format specified in Table 3.1. Moreover, an acceptable password for an account must also satisfy the following requirements:

1. Not be a password that is one of the three (3) most recently used passwords for that account
2. Must not be derived directly out of user's Personally Identifiable Information (PII) such as part of the name, birth year, phone no, index no, or program being followed
3. Must not be a word related to the University or department such as Moratuwa, UoM, mrt, Mora, or Katubedda
4. Must not be a dictionary word, slang, dialect, or jargon

All information systems should be configured to enforce all initial and renewed passwords satisfy this policy.

Table 3.1 - Password complexity matrix.

Account Type	Minimum Length	Combination	Change Frequency	Reset Mechanism
Faculty and administrative staff member	8	At least 1 uppercase (A-Z) and one lowercase (a-z) character, 1 number (0-9), and 1 symbol	3 years	Self-service reset via MIS if valid mobile and secondary e-mail are set up at the time of registering. At service desk with Photo ID or on written request of user and approved by Head of department/division
Undergraduate student accounts			Not required	Self-service reset via MIS if valid mobile and secondary e-mail are set up at the time of registering. At service desk with Photo ID
Postgraduate student accounts				
Visitor accounts including visiting lecturers			Annual	Self-service reset via MIS if valid mobile and secondary e-mail are set up at the time of registering. At service desk or on written request of respective Head of department/division
Role and task specific accounts			180 days	On written request of respective head of department
Event and project specific accounts				

Systems Administrators	12		Annual	At service desk with Photo ID or on written request of user and approved by Head of department/division
Systems Accounts / Superuser User			180 days	By superuser
Passwords used to protect encryption keys	15		Annual	

3.2 Initial Passwords

When a user account is created the user should be given a random password as per the password complexity defined in Table 3.1. Users should be prompted to change this password at the time of the first login to the respective system. The initial/first-time password should expire in 72 hours. If the user does not login within 72-hours from the generation of new password, account should be automatically disabled/locked. In such cases, user needs to request a new password following the procedure outlined in Section 3.4.

3.3 Transfer of Passwords

Newly generated passwords should be shared with the user only at the service desk, as a text message to his/her phone number, or e-mail. The phone number or e-mail should be the one specified in the user account request as per Section 2.2. No password should be shared with the user in the written form, and all forms of digital transmissions should be over an encrypted channel.

3.4 Changing Passwords

Depending on the account type information systems should prompt the user to renew the password as per the password change frequency defined in Table 3.1. Users may also change the password themselves from time to time, which is highly encouraged to keep the IT facilities secure.

In case a user has forgotten or lost the password, he/she could request CITeS and delegated administrators to reset the password. To reset a password should provide a valid photo ID such as the staff ID, student ID, and NIC to the service desk as specified in Table 3.1. Only the owner of a user account shall be allowed to request the password to be changed. The only exception shall be when the owner of the user account has been incapacitated or left the organization, in which case the relevant head of the department/division can request that the password is changed. For certain types of users, especially where a photo ID cannot be presented (e.g., role, task, event, and project-specific accounts) the respective Head of the department/division may request that the password is changed. In both the cases, the request must be either given in writing or should be initiated via the official e-mail address. The administration staff may reset the password only upon satisfactory confirmation of the photo ID or written request. In all cases, the renewed password should satisfy the password complexity matrix in Table 3.1 and should be treated similarly to an initial password and user shall be required to change their password at first subsequent login as outlined in Section 3.2.

3.5 Storage of Passwords and Other Credentials

All password and other credentials such as fingerprint data and digital certificates should be securely stored as per the details outlined in the Information Security Policy. Moreover, all passwords in digital form should be stored as one-way passwords that are hashed with a random salt. No password should be kept in clear text either digitally on in written form.

4.0 Supplementary Policies and Laws

This Policy is supplemented by following policies:

1. Information Communication Technology Policy
2. Acceptable Use Policy
3. Information Security Policy
4. e-Mail, Web, and Social Media Policy
5. Privacy Policy
6. ICT Operations Policy

These policies work and enforced together; hence, a specific case should be interpreted based on the combination of this Policy and all other applicable and approved policies. University community also needs to be aware of conduct which may breach national laws and lead to civil or criminal legal proceedings and penalties for which they will be held personally responsible. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017

5.0 Enforcement

The UoM reserves the right to withdraw the permission granted to any user or administrator to access IT facilities, if the user does not comply with this User Account and Password policy. Additionally, the UoM may take appropriate disciplinary, administrative, and legal action under the relevant rules and regulations against this policy violators.

6.0 Contact Information

Users requiring clarifications and feedback with regard to this Policy, subsequent policies, or those who wish to report a breach of this Policy should contact:

Director – Center for Information Technology Services (CITeS)
e-Mail: cites@uom.lk
Phone: 4400

Abbreviations

CITeS	Center for Information Technology Services
ID	Identity
HR	Human Resource
IT	Information Technology
LMS	Learning Management System (i.e., Moodle)
MIS	Management Information System (i.e., LearnOrg)
NFC	Near Field Communication
NIC	National Identity Card
PII	Personally Identifiable Information
UoM	University of Moratuwa