ICT Policy for Wachemo University

Prepared by

ICT Development Directorate

Policy Draft Submitted to Business Development Vice President Office

December 2021

Wachemo University

Executive Summary

This document lists ICT policies to abide by when using Wachemo University (WCU) ICT infrastructures, facilities, systems, services, equipment etc. The internal policies are adapted from various known universities around the world. The policies is customized by ICT directorate of wachemo university to suit its specific needs for managing resources and enforcing smooth ICT access and use at the institutional levels.

Internal ICT policies are essential for a smooth functioning ICT environment. WCU is generally required to develop Acceptable Use Policies (AUPs) for the ICT services. There has been a move away from writing short and simple AUPs towards developing full-fledged ICT policies for covering the aspects of infrastructure, applications, security, disaster recovery, business continuity, procurement, property disposal, internet use, email use, web content, research and learning application requirement etc in each campus.

So WCU is fully integrating policies into a wide range of services for students, faculty, administrators, and external users by focusing this policy. Based on this, the primary building block of preparing this policy is to ensure that students, academic staffs, and administrative staff take responsibility of their actions.

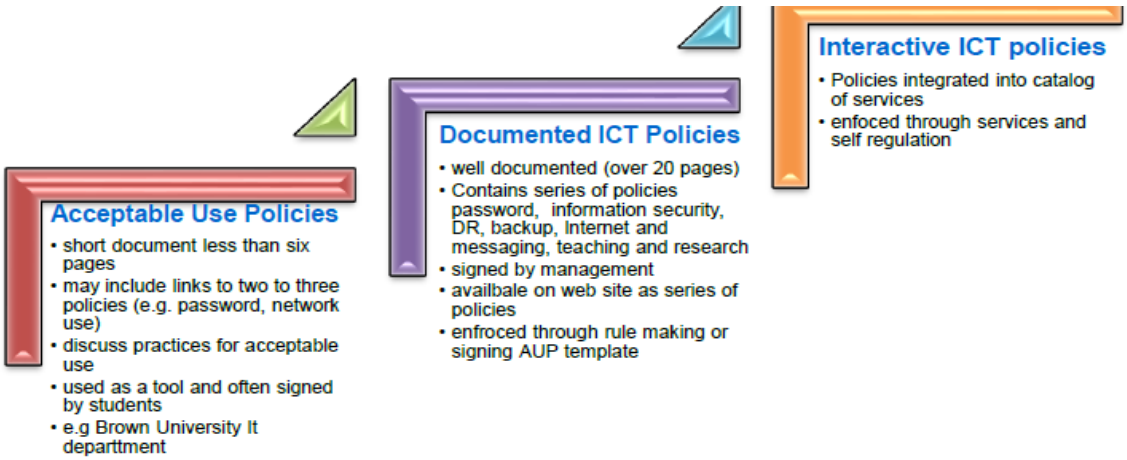

Figure 1 Trend of Development in ICT Policies in Higher Education Institutions

ICT policies for Wachemo University generally concern the following areas:

- Academic: services, teaching and learning support,
- Research support,
- Enterprise applications and information management,
- Digital content and library systems,
- Information security

- Infrastructure and network operations,
- Governance, management, customer services and support

The following internal ICT policies are proposed to be adopted by the ICT policies for Universities in Ethiopia.

Area of ICT Functions	
Academic Services: Teaching and Learning Support	• Virtual Learning Environment Policy • Plagiarism software use Policy • Video Conferencing Use Policy
Research support	• Research support policy • Research Data Management Policy • Identity Management Policy
Enterprise Information Management	• Information/Data Classification Policy • Website and Portals Policy • Social Media Policy • Application Development Policy • Software Compliance Policy • Database Management Policy
Digital Library System	• Digital Collection Policy • Digital Preservation Policy • Open Data Policy
Information Security	• Information security policy • Physical security policy • Disaster recovery policy • ICT incident reporting policy • ICT breach management policy • ICT monitoring policy
ICT Infrastructure Operations	• ICT Products and Services Procurement Policy • University Telecommunications Policy • Hardware Policy • Data Center Policy • Server Accessibility and Standards Policy • Bandwidth Use Policy • Cloud Policy

	• ICT Equipment Maintenance Policy • ICT Disposal Policy • Public Use Equipment Policy
Governance, Management Customer Services and Support	• General Internet Access and Use Policy • Backup Policy • Password Policy • Email Policy • Antivirus Policy • Bring Your Own Device Policy • User Support Policy
Academia versus ICT Collaboration	• Internship Policy • ICT Academies Operation Policy • Training, Consultancy and Research Collaboration Policy

In addition, policies often include statement of enforcement and accompanying tools such as "do" and "don't" posters and user agreements. The model policy for Wachemo University is provided in Appendix A.

Contents

1. Introduction to ICT Policy brief

Wachemo University (WCU) in Ethiopia has been growing fast in the recent years. The Government of the Federal Democratic Republic of Ethiopia has also invested in the ICT to support teaching, learning, research and management at universities. The Government has developed an education sector strategic roadmap with the intention to promote access, equity, quality, and relevance of higher education centered on better student outcomes. The [A] University recognizes ICT as prime mover and driver in promoting quality teaching, research, and administration. The performance and visibility of the University is determined to a great extent by its ICT infrastructure and applications towards improved student-centered learning. The University has taken the initiative of developing and regularly reviewing an ICT policy that will guide in the design, development, implementation, and effective use of the ICT services and resources.

1.1. Purpose of ICT policy

The policy defines the responsibilities of users of the University's ICT Infrastructures and services deter unacceptable ICT use by declaring the punitive actions, foster better service quality and fair use. The purpose of the ICT policy is to:

- Promote ICT use for teaching, learning, research and administration,
- Provide impetus for ICT application in libraries,
- Ensure smooth operations of ICT infrastructure, provide optimal bandwidth and access to Internet,
- Encourage the development and shared use of digital content,
- Guide the process of enhancing user utilization of ICT resources through training
- Standardize the ICT procurement and maintenance process
- Enforce and ensure minimum information and network security standards to prevent any misuse from its own users and outsiders,
- Promote good ICT governance, management, and support.
- Standardize ICT Infrastructure and application of the University
- Strengthen and institutionalization of ICT academy and Collaboration
- Provide ICT Training, Consultancy and Research

1.2. Applicability of the Policy

This policy applies to all the community of Wachemo University using computing and network resources. These include:

- Users (students, academic staff, professional and support staff, management bodies, external researchers, and guest lecturers) using either personal or University's provided equipment connected locally or remotely to the network of the WCU.
- All ICT equipment connected (locally or remotely) to wcu servers,
- ICT systems owned by and/or administered by the ICT Directorate
- All devices connected to the University network irrespective of ownership,
- Connections made to external networks through the University network,
- All external entities that have an executed contractual agreement with the University.
- All Infrastructures initiation, construction, expansion, and maintenance (ICT infrastructure, building and road construction, facility provisioning) across university premises

1.3. Approval of Policy Document

This policy document was discussed and approved for productive use by the University

Senate in date of _____

Signed: _____

2. ICT Polices for Learning and Teaching

2.1. Virtual Learning Environment Policy

Virtual Learning Environment (VLE) supports the development of technology-enhanced learning across both online and face-to-face teaching environments. VLE assists in: (i) enhancing the students experience (ii) supporting innovative teaching strategies, and (iii) building a digital capacity.

Rationale of the VLE Policy

The VLE policy is designed to ensure that every registered student has online access to an open standard Learning Management System (LMS), online teaching tools, and learning resources. The policy also designed to support university in their adoption of Learning Management System and online teaching tools for academic practices.

Scope of the VLE Policy

This policy applies to credit bearing modules and programs delivered to registered undergraduate and postgraduate students. The policy applies to the institutional VLE with regard to teaching and learning activities.

2.1.1. Policies

2.1.1.1. A single Institutional VLE that embodies Learning Management System and Online teaching tools will be used across all foundation, undergraduate, and postgraduate programs. This implies that the university will adopt a standardized open Learning Management System and online teaching tools across its programs, campuses, and branch colleges to ensure seamless VLE environment.

2.1.1.2. Open source and open standard e-learning systems and online teaching tools will be used to reduce cost and also allow for customization. The VLE will have the following features:

2.1.1.3. The minimum defined standard within the institutional Learning Management System include:

1. User friendly.
2. Open architecture features that support third party add-ons.
3. Scalability and modularity that allows for growth of content.
4. Support to multi-user access from many students and other users.
5. SCORM compliant1;
6. Good security features that allow for different levels of security.

7. Support assessment that are easy to update by lecturers; and features for testing online with effective results summary and feedback.

8. Support report generation

1. Module information, including course and module handbooks, module specifications, outline, key calendar dates and information regarding assessment. This information will be made available at the commencement of the module.

2. Lists of information resources/reading lists, such as books, journals, databases, web sites.

3. Lecture materials, before or after lecture, as determined by the lecturer.

4. Information on staff availability and communication.

5. Each module home page will contain information which is standardized and formatted for every module and the VLE interface will be structured to provide access to resources based on simple login and the minimum of navigation.

6. All digital materials used in the teaching and learning on the program will, where possible, be made available to the students within the VLE.

2.1.1.4. Information and Data Compliance

1. All users of the institutional VLE must comply with the Higher Education Intellectual Property Policy and the national copyright legislation.

2. Any learning and teaching content provided in an electronic format should be uploaded into an appropriate place within the VLE module in compliance with the [A] University Intellectual Property Policy,

3. In accordance with the higher education responsibilities under the Data Protection Policy student personal data must not be stored and/or maintained in third party hosted services where it may be at risk of being compromised unless approved by the Academic Registry and the University President.

2.1.1.5. Ownership and Implementation of the VLE Policy

1. The vice president for academic affairs will be the owner of this policy,

2. The Director of Information and Communications Technology directorate is responsible for technical service standards and management of the contract with an open VLE supplier.

2.1.1.6. Role of Faculty

The faculty of the University [A] should:

- o Prepare e-courses and upload to the VLE
- o Achieve a minimum level of proficiency in using VLE tools including Learning Management Systems and online teaching tools,
- o Ensure the learning content is uploaded to the university VLE,
- o Interact with students on timely basis to promote smooth online learning environment.
- o Proper utilization of ICT resources

2.1.1.7. Role of Department Heads

- o Make sure that staff are well trained on VLE
- o Follow up e-learning progresses

2.1.1.8. Role of Students

Students pursuing online learning environment either within campus or by distance learning will be are required to take the following into consideration.

- Read the course syllabus thoroughly and understand the course expectations,
- Set a realistic schedule and ensure regular study time,
- Set goals and deadlines to meet assignment due dates.
- Organize study schedule and create an electronic or weekly calendar and set reminders,
- Stay in touch with the faculty and know their preference on how and when they prefer to be contacted via phone, text, email, online office hours, messenger, or skype,
- Take time to evaluate progress by checking and calculating own grades,
- Plan time wisely and ensure time to study for test/quizzes,
- Connect with classmates to create an engaging productive environment,
- Discuss progress with faculty and keep track of deadlines and submissions,
- Login to the online environment regularly (at least daily) and complete assignments on time.

2.1.1.9. Role of ICT directorate

The ICT director of the Wachemo University should:

- Train staff on the use of VLE
- Prepare video tutorials on how to use VLE
- Ensure existence of required bandwidth, storage, up to date (latest) VLE

References and Sources:

University of Dublin VLE policy, https://www.tcd.ie/teachinglearning/assets/pdf/academicpolicies/VLE_Policy.pdf

- University of Wolverhampton, Virtual Learning Environment Policy, https://www.wlv.ac.uk/media/departments/office-of-the-vice-chancellor/documents/VLE-Operational-Policy-v_5.0.pdf
- University of Warwick, Virtual Learning Service Policy, https://warwick.ac.uk/services/its/about/policies/vle-service.pdf

2.2. Anti-Plagiarism Software Policy

This policy presents guidelines on the use of anti-plagiarism software to improve the integrity of students' and researchers' work at the Wachemo University. Most of the students work assignments or thesis is presented in paper format. It is a difficult task for the faculty to countercheck for plagiarism from paper-based submissions. This then leaves a doorway for dishonesty and by extension, poor quality and undeserving graduates.

The Wachemo University recognizes that use of electronic means to track plagiarism is an important element of the integrity in teaching, learning and research environment.

Rationale and Guidelines for Use:

- The primary purpose for the use of any plagiarism prevention software such as Turn it in at the Wachemo University is educational.
- Through plagiarism detection software, the Wachemo University is providing a means by which faculty can help students enhance their understanding of academic integrity and plagiarism. The adoption of the program is intended to encourage honest work by making it essential for students to reflect on the authenticity of their assignments.
- Anti-plagiarism software will also be used to assist with plagiarism detection where there is concern that an assignment or research work contains plagiarized material.
- Staff and students should be aware that anti-plagiarism software is not the only method of checking for plagiarism and other means are readily available. Students and researchers cannot use plagiarism detection software to prove that they have not plagiarized. Such judgments need to be made by individual faculty, faculty members, advisors, examiners, or editors in reference to institutional plagiarism detection policy.

2.2.1. Policies

2.2.1.1. This Policy should be read in conjunction with the Wachemo University Plagiarism policy, which is developed and widely available through students' Handbook.

2.2.1.2. All students are expected to adhere to the highest standards of personal honesty and integrity in their work. Submissions to faculty must be original or respect the intellectual contributions of others through correct referencing.

2.2.1.3. The Wachemo University has adopted a common anti-plagiarism software tool, which is used by most of the universities in Ethiopia. Anti-plagiarism compares assignments against its international database and produces an originality report. This identifies the percentage of text (excluding that in quotation marks) which can be matched to any of the existing data, either as identical text or closely paraphrased material.

2.2.1.4. The Wachemo University recognizes that students may duplicate assignments that are not readily available in international databases for example those produced by different universities in Ethiopia. Anti-plagiarism Tool2 will therefore be trained to cover searches on the national repositories.

2.2.1.5. The University's guidance is for the assignments of every course to be submitted to Turn it in whenever appropriate. This will ensure the right of the originator of ideas in every assignment so it will not be plagiarized by others.

2.2.1.6. In alignment with the principle of using Anti-plagiarism Tool primarily as an educational tool, students should be allowed to submit their assignments once and review the similarity report prior to the final submission of the assignment. This formative approach provides students with the opportunity to identify potential problems and seek advice as appropriate.

2.2.1.7. The University faculty should acquaint themselves with usage of the anti-plagiarism software and required to ensure that no final marks are awarded before plagiarism is tested.

2.2.1.8. The faculty should use the similarity reports generated for their course assignments to help identify potential instances of student plagiarism and take appropriate follow-up action as per the University's anti-plagiarism policy.

References:

• University of Glasgow. Policy for the use of the Plagiarism Prevention Software, https://www.gla.ac.uk/media/media_105133_en.pdf

• Hongkong Baptisi University, Anti-plagiarism software policy, https://chtl.hkbu.edu.hk/elearning/documents/SenateApproved-Guidelines-AntiPlagiarismSoftware.pdf

2.3. Video Conferencing Use Policy

The Wachemo University believes that students need a touch of the face-to-face lectures from the lecturers and professors. At the same time, the University seeks to exploit video conferencing capabilities of the web and other technologies so that lectures can be taken from lecturers at distant locations anywhere in the world. Video conferencing is also important to virtual classroom participation, student consultation, thesis/dissertation defenses, administration duty of institute, multi-site meetings, and project collaboration

The Wachemo University recognizes video conferencing as part of the e-learning infrastructure. The operation of video conferencing should meet the following policy guidelines.

2.3.1.1. The video conference at the university will be used for educational purpose only.
2.3.1.2. The recordings of the lectures during the video conferences are subjected to copyright law
2.3.1.3. The video conferencing service is available to faculty, staff, and students of [A] University.
2.3.1.4. Video conference services will not be used for personal calls.
2.3.1.5. Outgoing video calls will be covered by the University,
2.3.1.6. ICT directorates provides the technical support for video conferencing equipment and ensure that they are in functioning order,
2.3.1.7. Video conferencing services will only be available through booking the services using a video conferencing request form.

2.3.1. Policies

References

• http://med.stanford.edu/edtech/services/ClassroomTechnologies/video-conferencing-policy.html

3. ICT Polices for Research

3.1. Research Support Policy

The Wachemo University upholds a high standard of research and encourages faculty and researchers to leverage Information and Communication Technologies to advance their research. The Information Technology directorate will provide specialist services to all researchers regardless of the field and the stage of research in collaboration with faculties and the researcher. The University will strive to make the following services available to researchers:

- High-quality data storage services for fast access or large data sets,
- Computers for fast calculations, advanced simulations, and big data analysis,
- Access to science gateways, massive storage, and shared workflows,
- Visualization facilities and services to help understand advanced simulations and big data

3.1.1. Policies

3.1.1.1. The Wachemo University will provide research technology support that will collaborate with research faculty, staff, and graduate students to help overcome technical obstacles to effectively use computational resources for research. The following support will be provided for all skill levels and for all areas of research within the University

3.1.1.2. Research Computing Resources

- Matching computing, software, and data storage resources to research needs,
- Assisting in integrating computational components into a study to best address research questions.
- Provisioning of discipline specific licensed software for researchers (students and staff)

3.1.1.3. Visualization

- Creating custom images, movies, or interactive visualizations for publication and exploratory analysis.
- Improving the clarity and impact of publication graphics, tables, and charts.

3.1.1.4. Data Science Support

- Planning and setting up computing and data workflows for research projects
- Automating repetitive research tasks.
- Designing databases and other data management solutions.
- Overcoming other data challenges or technical obstacles to a research.

3.1.1.5. Cloud Computing Services

3.1.1.6. Training

- Conducting workshops on high performance computing, statistical software, computer programming, computing tools for researchers, research replicability, data visualization, and data analysis.
- Workshops will be offered for both the University community and specific departments or groups.
- Providing training and consultation on cloud services, tools, and practices.
- Providing access to cloud-based computational resources and software to run your analysis at scale.

References

https://www.it.northwestern.edu/research/consultation/index.html

3.2. Research Data Management Policy

Introduction

There is growing recognition that the maintenance of accurate and retrievable data arising from research projects is an essential component of good practice in the conduct of research. The University considers that the appropriate and accurate management of research data to be a key component of research integrity.

Expectations

Research data should be:

- Accurate, complete, authentic, and reliable.
- Identifiable, retrievable, and available when needed.
- Secure and safe.
- Kept in a manner that is compliant with legal obligations and, where applicable, the requirements of funding bodies and project-specific protocols approved by the University Ethics committee or an equivalent body of the university research management.
- Able to be made available to others in line with appropriate ethical, data sharing, and open access principles

3.2.1. Policies

3.2.1.1. Research data arising from publicly funded research should be treated as a public good and made available to others wherever possible.

3.2.1.2. Data should be stored in a secure data repository suited to the data concerned.

3.2.1.3. Data should be retained for a period which follows best practice in the discipline or funder requirements. If none exist, data will be retained by default for a period of 10 years after which a review takes place in deciding whether the data is worth keeping for longer.

3.2.1.4. Responsibility for research data management through a sound research data management plan during any research project or program lies primarily with the researchers. Researchers are responsible for:

- Managing research data and records in accordance with the principles and requirements set out in the expectations of this policy,
- Data management plan at the outset of a research project, which should be documented with clear procedure for the collection, storage, use, re-use, access and retention or destruction of the research data,
- Planning for the ongoing custodianship of their data after the completion of the research,
- Ensuring that any requirements in relation to research data and records management placed on their research by funding bodies or regulatory agencies or under the terms of a research contract with the University are also met.

3.2.1.5. All new research proposals [from date of adoption] must include research data management plans or protocols that explicitly address data capture, management, integrity, confidentiality, retention, sharing and publication

3.2.1.6. The University will be responsible for:

- Providing training, support, advice and where appropriate guidelines and templates for the research data management and research data management plans.
- Providing access to services and facilities for the storage, backup, deposit and retention of research data and records that allow researchers to meet their requirements under this policy and those of the funders of their research.
- Providing mechanisms and services for storage, backup, registration, deposit, and retention of research data assets in support of current and future access, during and after completion of research projects.

3.2.1.7. Any data which is retained elsewhere, for example in an international data service or domain repository should be registered with the University.

3.2.1.8. Research data management plans must ensure that research data are available for access and re-use where appropriate and under appropriate safeguards.

3.2.1.9. Research data of future historical interest, and all research data that represent records of the University, including data that substantiate research findings, will be offered, and assessed for deposit and retention in an appropriate national or international data service or domain repository, or a University repository.

3.2.1.10. Exclusive rights to reuse or publish research data should not be handed over to commercial publishers or agents without retaining the rights to make the data openly available for re-use unless this is a condition of funding.

References

University of Edinburgh, Research Data Management Policy, https://www.ed.ac.uk/information-services/about/policies-and-regulations/research-data-policy

University of Brighton, Research Data Management Policy, https://staff.brighton.ac.uk/mac/public_docs/Policies/Data%20Management%20Policy%20final%20(v5).pdf

University of Aston, Research Data Management Policy, https://www.aston.ac.uk/EasySiteWeb/GatewayLink.aspx?alId=315281

4. Identity Management Policy

Introduction and Rationale

A growing number of educational resources and services are offered on-line, and users (students, faculty, researchers, staff, alumni, or others) increasingly expect access to these resources from various locations, including mobile devices. Identity management allows institutions to provide this access in a reliable, secure manner without a proliferation of credentials. To the extent that federated identity allows institutions or even individual faculty to easily offer controlled access to research data or other resources, it has the potential to enable new levels of academic collaboration. Identity management can support institutional policies for extending access to valuable resources to certain groups of users.

4.1.1. Policies

4.1.1.1. The Wachemo University uses a single identifier (user ID) for use by all University systems as the basis for user authentication. This identifier is created by a central identity management system.

4.1.1.2. The Information and Communications Technology Directorate is responsible for the operation, management and oversight of the Identity and Access Management (IAM) Program, which assigns and manages official identities for the University. IAM is critical to ensuring that unauthorized access to information, systems, applications, and physical areas is prevented, along with potentially fraudulent activity. This includes the assignment of the individuals' User ID numbers, and email addresses.

4.1.1.3. The university employee, student or affiliate using a university-owned workstation, computer or device connecting to university's network (wired or wireless) to access a restricted resource must use the university Login credentials (user ID) as provided through a recognized directory service.

4.1.1.4. Any university employee, student or affiliate authenticating to a university-restricted software service must use university Login credentials (user ID).

4.1.1.5. All students, employees and affiliates are responsible for safeguarding their university user ID credential as defined in the Acceptable Use of Data and Technology Resources Policy and Sensitive Data Protection Policy.

4.1.1.6. University management processes ensure that user IDs are never reused. The application software system should make no assumptions about the format or length of the user ID, as it may be either a short alphanumeric string or a complete email address. The vendor must specifically highlight any restrictions its software places upon the identifying token.

4.1.1.7. The University requires that all new software systems acquired and deployed use the user ID to identify users.

4.1.1.8. Authentication of users must use the user ID and its associated password. The University will not manually assign other user identifiers and/or passwords within a specific software system.

4.1.1.9. The University will not bulk transfer groups of user's user IDs into software systems in order to pre-populate a user profile database.

4.1.1.10. The University makes available four authentication methods for use by software applications.

a. Web Single Sign-On (via Forgerock OpenAM, for instance)

b. LDAP (via Oracle DSEE , for instance)

c. Microsoft Active Directory (via Windows Server, for instance)

d. Federated authentication (via SAML)

4.1.1.11. Due to privacy regulations, the University closely monitors how information is collected, stored, exposed, and used in its academic, research, and administrative processes.

4.1.1.12. All services outside the University must be accessed through the Web. Federated authentication is the preferred method for authenticating and authorizing users. The University will not expose any other authentication method outside of its network.

4.1.1.13. The University supports federated authentication using software. The software should describe any and all federation protocols the system or service will support.

4.1.1.14. If federated authentication is not possible, then authenticated access should rely upon a secure session-key technology to designate a persistent session with the service point. Because session-key techniques must be coordinated, any aspect of a proposed software system or service that requires such accommodation must be clearly called to the University's attention for evaluation.

4.1.1.15. The University does not export or bulk transfer identities, passwords, or personal information to third parties for authentication or any other purpose.

References

- North-western University Identity and Access Management Policy, https://www.it.northwestern.edu/policies/bid.html
- Boston University, Identity Management Policy, http://www.bu.edu/policies/information-security-home/data-protection-standards/identity-and-access-management/
- West Virginia University, Identity and Access Management Policy, https://it.wvu.edu/policies-and-procedures/security/identity-and-access-management-policy

8. Infrastructure Policies

8.1. ICT Products and Services Procurement Policy

The purpose of this policy is to provide a framework for the procurement of all ICT products and services such as ICT infrastructure, facilities, systems, services, tools, hardware, software, license keys etc. and any externally hosted systems or software for the University.

The University has agreed standards in place for infrastructure, systems, services, computer software, operating systems, networks, hardware, and peripherals. The main benefit of standardization is:

• ICT Directorate' Staff are familiar with infrastructure, systems, services, hardware and peripherals, thus speeding up fault finding (analyze and troubleshoot unserviceability)

• ICT Directorate' is able to stock standard spares in order to reduce down time,

• ICT infrastructure and facilities, systems, services, software and hardware installations and implementation are planned and coordinated centrally by experienced engineers/experts,

• ICT staff with relevant skills and experiences are placed, transferred, promoted, and recruited.

8.1.1. Policies

8.1.1.1. ICT Products, Services and Software Procurement Guidelines.

1. The ICT Directorate' is the sole authority for placing orders for ICT Products, Services, software and licenses on behalf of the University regardless of the source of funding. The centralization will enable the following:

- brand and model standardization and interoperability where appropriate,

o campus-wide inventory of non-capitalized infrastructure, facility, systems, services hardware, software and license keys to facilitate effective planning, maintenance, upgrades, and disposal,

o pricing advantages obtained through volume purchasing and working with preferred vendors,

o license compliance for software procurements , and

o ensure that hardware and software will be compatible with ICT infrastructures, facilities, systems, services, and software

All ICT products and services related procurement will need to have full approval and authorization prior to requisitioning.

3. All ICT products and services related hardware and software will be specified by the Information and Communications Technology Directorate software and/or hardware management team.

4. Hardware and software cannot be purchased and procured without approval by ICT Directorate.

5. All requests for procurement of ICT products and services , whether as individual items or as part of a larger project, must be sent to the ICT Directorate who will process the request as per the ICT Directorate' regulations (standards and conformity) and procedures.

6. ICT Directorate' will make a decision whether to approve, decline or amend the specification of requirements for the procurement of ICT products and services:

7. If ICT products and services is declined or changed, ICT Directorate' will provide a brief explanation to the requesting manager for the decision.

8. ICT Directorate' will keep the customer informed of the decision and the outcomes if ordered.

9. If ICT products and services are approved or changed then ICT Directorate' will order the equipment directly with suppliers.

10. Where ICT products and services are authorized and ordered, an installation window will be proposed, however this may change according to ICT priorities.

11. The ICT Directorate' must have a standard set-up procedure for new ICT products and services. This procedure ensures the equipment is configured correctly and that all IT security measures are addressed. This includes the setup of passwords, anti-virus software and security marking the equipment and adding the university asset management database etc.

12. The Information and Communications Technology Directorate will not install software or hardware unless it has been involved in the specification of both. Hardware and software cannot be installed by non-Information and Communications Technology Directorate staff on university premises.

13. The Information and Communications Technology Directorate will ensure that all of the University's ICT policies, procedures are abided when setting up software and hardware.

14. ICT Equipment replacement will be given priority over new equipment in order to maintain continuity in the existing service. 8.1.1.2. External ICT Services Procurement Guidelines 8.1.1.3. Large Scale ICT Products and Services Procurement

1. External IT Services include: Professional services, Cloud services, hosting of software, accessing third party software (except via the internet), maintenance / support services and any other third party supplied ICT related service including consultancy.

2. All requests for External ICT Services must be sent via the ICT Directorate. The Information and Communications Technology Directorate is the sole authority for placing orders for External ICT Services acquisition.

3. ICT Directorate' will make a decision whether to approve, decline or amend the requirements for purchasing of these services. If external ICT Services are declined or changed,

4. ICT Directorate will keep the customer informed of the decision and the outcomes if ordered.

1. Procurement involving substantial ICT investment (>200,000 Birr, based on procurement regulations and procedures) must be authorized by the University Endorsing Committee and top management as well as University Executive Management. Large scale ICT products and services procurement shall be overseen by ICT Steering Committee /ICT Executive Management Committee /ICT Advisory Council.

2. In large project cases the Information and Communications Technology Directorate must be represented on any project program board for investments of this nature.

References

• Michigan Technology University, Information Technology, Software and Hardware Purchase Policy, http://www.mtu.edu/policy/policies/finance/2-14/2-14-1/

• Trinity University, Computer Purchase and Replacement Policy, https://inside.trinity.edu/information-technology-services/information-technology-policies/computer-replacement-purchase-policy

• University of Salford, Information Technology Procurement Policy, https://www.salford.ac.uk/__data/assets/pdf_file/0011/898436/ITProcurementPolicy.pdf

8.2. Public Use ICT Equipment Policy

This policy governs the registration and operational management of public use ICT equipment such as switches, access points, surveillance cameras, access control terminals, electronic time attendance terminals, mounted LCD projectors, digital signage solution screens, smartboards, network cabinets and racks, uninterruptable power supplies, power systems installation appliances and ICT related public use equipment.

The Public Use ICT equipment includes but not limited to the followings:

• WAN, LAN, WLAN equipment, Surveillance System equipment

• Computers and accessories for computing and internet service facilities

8.2.1. Policies

8.2.1.1. Public Use ICT Equipment Responsibilities:

1. Property Administration Directorate in consultation with ICT Directorate shall classify and categorize ICT equipment as inventories (consumables and replacement accessories), fixed assets, public uses.
2. Property Administration Directorate shall register and administer ICT equipment used for public services provision as public use ICT equipment
3. ICT Directorate takeout ICT consumables, ICT fixed asset equipment and Public Use ICT equipment
4. ICT shall monitor and operationally management functioning ICT Public Use equipment
5. University Security and Safety Directorate/Campus Police Department shall carefully safeguard and oversee Public Use ICT equipment on daily basis
6. University Security and Safety Directorate/University Campus Police Department shall notify and report any encountered incidents as well as execute and flow up the legal actions.

8.2.1.2. Modifications

1. All Public Use ICT equipment modifications, replacement, upgrade must be implemented and coordinated through the ICT Directorate
2. Only the ICT Directorate' approved contractors and or third-party are authorized to replace, upgrade modify Public Use ICT equipment

8.2.1.3.Access Public Use ICT Equipment

1. Access to public use ICT equipment is restricted to ICT Directorate' staff.

8.2.1.4. Disconnection

2. Any public use ICT equipment, accessories and materials which interferes or identified as security risk on operation of the network infrastructure shall be logically or physically disconnected from the infrastructure by ICT Directorate' staff.

8.2.1.5.Logging of Use

1. The University may maintain logs of data for management, service rectification and accounting purposes without infringing the privacy rights of individual users.

8.3. Network Infrastructure Policy

This policy governs the development and operational management of the University network infrastructure. Access to the University's network infrastructure is available to staff, students and in some case external users. All users of the University's network infrastructure should be aware of their responsibilities as described in the Acceptable Use of Information Technology. The University network infrastructure includes but not limited:

• The inter-building and intra-building wired or wireless communication systems up to and including the "network socket outlet on the wall",

• The devices that route and manage the communication of data, video, and voice signals, including perimeter and interior firewalls, routers, switches,

• Telephone handsets, voice mail servers, and wireless network base stations and access points, and

• The inter connections to and from voice and data networks external to the University.

8.3.1. Policies

8.3.1.1. Network Infrastructure Development and Operational Management Responsibilities:

The Information and Communications Technology Directorate is responsible for:

1. Designing, installing, documenting, monitoring, maintaining, and supporting the IT network (including the wireless network),
2. Determining standards for equipment suitable for connection to the University IT network,
3. Managing University wide agreements which permit interconnections to and from voice and data networks external to the University,
4. Ensuring compliance with telecommunications and other relevant legislation,
5. Providing a guaranteed dial tone for emergency telephones and systems, building management systems, fire monitoring systems, and security telephones,
6. The management of IP address spaces (public and private), telephone extension number allocation and wireless radio frequency spectrum and SSIDs, and
7. The provision of remote access services (including VPN, dial up modems and remote access servers) which permit access to the University's Information Technology facilities from offsite locations. 8.3.1.2. The construction project office of the university is responsible for:

1. New buildings, buildings expansion, renovation and partitioning construction civil works shall incorporate Network infrastructure design and implementation.
2. Road construction and facilities provisioning civil works in university premises must be executed in official consultation and consensus with ICT Directorate prior to design and implementation

3. Campus Network infrastructure and buildings network infrastructure architectural design shall be incorporated with campus master plan and buildings master design, respectively.

8.3.1.3. Modifications

1. All cabling modifications or additions to the IT network must be coordinated through the ICT Directorate' to ensure they comply with national, state and local codes as applicable to wiring methods, construction and installation of data and communications cabling systems, and equipment.
2. Only the ICT Directorate' and approved nominated contractors are authorized to place equipment or cabling in wiring closets, equipment rooms, etc.
3. Users must not make any modifications to the IT network. Only wireless networking equipment installed and managed by the ICT Directorate' is allowed to be connected to the University IT network.
4. Where existing equipment needs to be relocated, or new equipment needs to be connected, advice should be sought from the ICT Directorate' to confirm that the network connection point is
activated and suitable for the intended use, and that the new equipment is suitable for connection to the network.
5. Any device (hardware or software) which has the potential to interfere with the IT network must not be connected, installed or run on any computer connected to the IT network without the prior approval of the Director of ICT Directorate' or nominee.

8.5. Data Centre Policy

The Data Center is vitally important to the ongoing operations of the University. The following policies and procedures are necessary to ensure the security and reliability of systems residing in the Data Center.

Role Definitions

- Data Center Employee: Division of ICT employees who work at the Data Center
- Authorized Staff: University employees who are authorized to gain access to the Data Center but who do not work at the Data Center
- Authorized Vendor: All non-University employees who, through contractual arrangement and appropriate approvals, have access to the Data Center
- Visitors: All other personnel who may occasionally visit the Data Center but are not authorized to be in the Data Center without escort

8.5.1. Policies

8.5.1.1. Access to the Data Center

In order to ensure the systems housed within the data center are kept secure, the following policies apply to all personnel requiring access:

1. All personnel who access the Data Center must have proper authorization. Individuals without proper authorization will be considered a visitor.
2. Visitors to the Data Center must adhere to the visitors' guidelines.
3. Authorizations will be verified on a quarterly basis.
4. All personnel must wear a valid University or vendor identification badge at all times.
5. All personnel must sign in when entering the Data Center to document the time and purpose of their visit. They also must sign out when leaving.
6. All personnel must enter through the Data Center's north entrance and must wear a University ID or visitor's ID at all times.
7. Authorized staff will have access to the Data Center at any time.
8. Systems housed within the Data Center that contain classified as Level III or above will be monitored by Data Center employees through live video cameras.

8.5.1.2. Equipment in the Data Center

In an effort to maximize security and minimize disruptions, the following policies apply to all equipment housed in the Data Center.

1. A form must be completed for all equipment installations, removals, and changes.
2. Data Center employees will deny entry to authorized staff or vendors who intend to install, remove, or rename equipment without an accurate equipment form.
3. Equipment housed within the Data Center must meet certain system specifications.

8.5.1.3. Access Authorization

University staff members must be pre-approved for unescorted access within the Data Center. Vendor access must be sponsored by an authorized staff member, or a dean, director, or department chair. Authorizations will only be approved for individuals who are responsible for installation and/or maintenance of equipment housed in the Data Center. Approval processes are as follows:

1. Authorization forms must be signed by the dean, director, or department chair of the person requesting access.
2. After approval, the Division of ICT Services and/or Data Center manager will review and approve.
3. If approved, the authorized staff member or vendor will be added to the authorization database, and the authorization form will be kept on file.
4. Authorized staff/vendors will be allowed entrance into the Data Center by a Data Center employee but will then have unescorted access within the Data Center.
5. Authorized staff/vendors are responsible for logging in/out when entering/exiting the Data Center. The purpose of the visit must be documented.

8.5.1.4. Visitor Procedures

Anyone who is not a Data Center employee, an authorized staff member, or authorized vendor is considered a visitor. All visitors to the Data Center must adhere to the following procedures:

1. All visitors must enter through the main entrance of the Data Center.
2. Visitors must be accompanied by either a Data Center employee or other authorized staff member at all times while in the Data Center.
3. Visitors must log in/out when entering/exiting the Data Center. The purpose of the visit must be documented.
4. Visitors must wear a visitor's badge at all times.

5. Visits should be scheduled through the Data Center manager at least 24 business hours in advance. Unscheduled visits to install equipment or perform other tasks may be turned away.

8.5.1.5. Audit Procedures

1. The ICT Directorate' will send a list of authorized staff and authorized vendors to the appropriate dean, director, or department chair on a quarterly basis (January, April, July, and October) for review and verification.
2. Each dean/director/department chair will review and update the list of authorized staff/vendors and return it to the Data Center manager within two weeks.
3. Failure to return access audits will result in revocation of access privileges for previously authorized staff/vendors until such time as the audit is returned.

8.5.1.6. Equipment Installation

Authorized staff performing the installation must submit an installation form.

8.5.1.7. Equipment Removal

Authorized staff performing the removal must submit a removal form.

8.5.1.8. Equipment Renaming

Authorized staff performing the rename must submit a renaming form.

References

• West Virginia University, Data Centre Access Policy, https://it.wvu.edu/policies-and-procedures/security/data-center-access-policy

• University of Missouri, Data Centre Policy and Procedures, https://doit.missouri.edu/about/policies-procedures/data-center-policies-procedures/

• George Mason University, Data Center Operational Policy, https://itservices.gmu.edu/policies/upload/ADC0D1-Data-Center-Operational-Policy.pdf

8.6. Server Accessibility and Standards Policy

The purpose of these procedures is to describe special requirements for server management that apply to the Wachemo University.

All server administrators must comply with the University Security Policies outlined in Appendix A. The Information Technology Services will provide oversight and assistance for the entire campuses of the Wachemo University. The University will use virtual server infrastructure to improve backup, disaster recovery, and system administration.

Server Registration, Inventory, and Deregistration

The Information and Communications Technology Directorate is responsible for maintaining a list of all campus servers belonging to the University. In order to facilitate the maintenance of this list, **System Administrators** must register their servers with the IT Services Department.

Server Security Standards and Processes

Server admins must review and comply with the security policies of the University. The **first thing** a system administrator must do is to review the types of data stored on each server administrated.

8.6.1. Policies

8.6.1.1. Servers are provided for the purpose of accomplishing tasks related to the university's mission.

8.6.1.2. Specific personnel will be identified for each of the following roles:

1. server owner,
2. server administrator,
3. security administrator. 8.6.1.3. Server owners must register their server with the University Information and Communications Technology Directorate Changes to server registration information should be promptly reported to the Information and Communications Technology Directorate

8.6.1.4. Prior to the purchase of any server, the server owner should contact the ICT Directorate' to evaluate the capabilities required to maintain server compliance and review alternative solutions where applicable.

8.6.1.5. Procedures for managing servers will vary depending upon the classification of the data stored on the server. Server administrators must review the Information Classification Policy of the University and classify data stored on the servers. Servers that store confidential data must be given extra security, and system administrators of such systems must ensure this.

8.6.1.6. Once the data security classification is complete, server administrators must review and comply with the University Security Policies.

8.6.1.7. System administrators must ensure that their systems comply with the applicable account provisioning standard prescribed by the ICT Services Department.

8.6.1.8. All servers must comply with the university authentication standards.

8.6.1.9. System administrators should use centralized identity management services, including university managed authentication framework like Shibboleth, Duo Two Factor Authentication, LDAP Authentication, and Eduroam.

8.6.1.10. Severs must be backed up according to the backup and disaster recovery and business continuity polices of the university.

8.6.1.11. Servers must employ device firewalls and in some instances network firewalls that meet the device firewalls and network firewall standards.

8.6.1.12. System administrators are responsible for ensuring that all servers under their control comply with the ICT Directorate' Log Management Standards.

8.6.1.13. Server storage must follow the Media Sanitization Standard before it can be recycled, sold, returned to the vendor, or leave the campus.

8.6.1.14. Servers must be configured to meet the Operating System Access Control Standard.

8.6.1.15. Servers that store private highly restricted data must be located in a secure physical facility managed by the ICT Services Department.

8.6.1.16. All servers must be patched to meet the Security Patching Standard.

8.6.1.17. All servers must comply with the Virus/Malware Protection Standard by ensuring that anti-virus software is installed and running.

8.6.1.18. The ICT Directorate' will conduct routine scans of the university server environment. Vulnerabilities will be communicated to the server owner and server administrator for resolution.

References:

• Lamar University, Server Management Policy, https://www.lamar.edu/it-services-and-support/policies/pdfs/IT%20Server%20Management%20Policy.pdf

• University of Minnesota, Server Management Procedures, https://itss.d.umn.edu/security-policies/policies-procedures/server-management

• University of Washington, Server Policy, http://www.washington.edu/admin/rules/policies/APS/17.01.html

8.7. Bandwidth Use Policy

The Wachemo University has substantial bandwidth capability on and off campus for its enterprise needs. However, in some areas, including dormitories, students continue to consume all of the capacity that we have been able to provide. There is a concern that high amount of traffic related to streaming video (e.g., Kana TV) running across our backbone segments during

prime academic hours. This policy aims to provide for an acceptable use of the bandwidth as a shared resource for academic needs.

8.7.1. Policies

8.7.1.1. If high bandwidth applications for recreational use of our network are identified, they will be restricted or blocked.

8.7.1.2. Services which can have a negative impact on the wired/wireless network include, but are not limited to:

1. streaming video,
2. Peer-to-Peer file sharing, and
3. Multiplayer Gaming and Game Servers.

8.7.1.3. Such services will be monitored for the impact on disruption on the bandwidth use for learning, teaching and research.

8.7.1.4. Students, faculty, and visitors must use the network for academic purposes, but not use it for financial gain, illegal purposes and transmitting large files that are not educational or copyrighted files.

8.7.1.5. Student and faculty may not operate a peer-to-peer (P2P) file sharing protocol on your computer. This includes the systems (among others): Kazaa, Morpheus, Direct Connect, LimeWire, Gnutella, eDonkey, BitTorrent, etc.

8.7.1.6. Student and faculty should aware that they are responsible for traffic generated by your computer. The University uses a bandwidth management policy which will effectively slow down your connection if you use more than your allocated quota.

8.7.1.7. All students, faculty, staff, and guests on the university network are allowed to use xx gigabytes a day and yy gigabytes a week, for individual use.

8.7.1.8. Students will be warned of excessive bandwidth use. Repeated excessive bandwidth use by students will be reported to the director of student services. The ICT Directorate' may quarantine the given device(s) (Computer, Game Console, Mobile, and/or Network Device), based on its IP address and the Director of Student Services will meet with the student to review what they were doing to exceed the bandwidth utilization thresholds, discussing issues related to stewardship, community, and legality if warranted.

8.7.1.9. Faculty will be warned of the excessive bandwidth use. Repeated excessive usage unless justified by valid academic reasons will be reported to the individual's Supervisor or the Vice President Business and Administration. The individual's computer system may be placed

into the quarantine network based upon interaction between Information Technology Service Department, the individual, and the supervisor as a result of the review process.

References

• Tyalor University, Bandwidth Utilization Policy, https://www.taylor.edu/dotAsset/11034dfb-112e-484e-98cf-1e108cbad6cb.pdf

• Robinson College, Network Usage Rules, https://www.robinson.cam.ac.uk/college-life/it/network-usage-rules

8.8. Cloud Computing Policy

Cloud computing is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, the University for services such as, but not limited to, social networking applications (i.e., blogs and wikis), file storage (assignment drop box), and content hosting (publishers textbook add-ons). This policy pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.

Cloud computing offers a number of advantages including low costs, high performance, and quick delivery of services. Cloud services support, among other things, communication; collaboration; project management; scheduling; and data analysis, processing, sharing, and storage. Cloud computing services are generally easy for people and organizations to use, they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones), and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to institutional networks, and raises concerns around privacy and security.

The following data are covered by this Policy:

• Student record data,

• Personnel data,

• Financial data,

• Student life data,

• Departmental administrative data,

• Legal files,

• Research data,

• Proprietary data, and

• Defined forms of data that pertain to or support the administration of the University.

8.8.1. Policies

8.8.1.1. Faculty, staff, and students must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice. Risks with using self-provisioned cloud services include:

o unclear, and potentially poor access control or general security provisions,

o sudden loss of service without notification,

o sudden loss of data without notification, and

o data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy.

8.8.1.2. The Wachemo University does not permit the use of public cloud storage for the University business information especially those treated as confidential, regulated, and administrative.

8.8.1.3. Use of cloud computing services for university purposes must be formally authorized by the Director of Information Technology Services and the University management. The Director of Information Technology Services will certify that security, privacy, and all other IT management requirements are adequately addressed by the cloud computing vendor.

8.8.1.4. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Director of Information Technology Services.

8.8.1.5. The Information and Communications Technology Directorate may use public cloud for institutional data that is wide and open distribution to the public at large.

8.8.1.6. The use of cloud services must comply with University existing Information Technology Usage Policy.

8.8.1.7. The use of cloud services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the University as a public institution.

8.8.1.8. Personal cloud services accounts may not be used for the storage, manipulation, or exchange of prohibited forms of communication or University-owned data.

8.8.1.9. Risks

The main risks when files are stored in public cloud storage are that:

1. The University can no longer guarantee the quality of access controls protecting the data,
2. The location where the data is stored may not be guaranteed as remaining in Ethiopia, and so may not meet national data protection requirements,
3. In many cases, public cloud storage requires that files be associated with an individual's personal account. Should that individual suddenly become ill, be absent for other reasons or leave the university, the University will lose access to the data,
4. Cloud services generally limit their liability for negligence, resulting in little or no recourse should the provider misuse, lose or damage information stored in the cloud,
5. few cloud providers guarantee they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights,
6. Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights,
7. Using cloud storage client software to synchronize files between work and personal devices could result in sensitive information being held inappropriately on personal equipment.

8.8.1.10. Exit strategy

1. Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans.
2. Staff and students are responsible for taking privacy and security into consideration when making decisions using cloud computing services.

References

• Cape Breton University, Policy on Cloud Computing, https://www.cbu.ca/wp-content/uploads/2015/07/Cloud-Computing-Policy-March-1-2015.pdf

• Kent State University, Cloud Computing Strategy, https://www.kent.edu/sites/default/files/file/KSU_Cloud_Strategy-V6-201706.pdf

• Tufts University, Cloud Computing Services Policy, https://it.tufts.edu/cloud-pol

9.2. Backup Policy

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. The Information and Communications Technology Directorate recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

The main purpose of this policy is to provide secure storage for data assets critical to the workflow of official university business, prevent loss of data in the case of accidental deletion / corruption of data, system failure, or disaster and permit timely restoration of archived data in the event of a disaster or system failure. To ensure server and data continuity and to support the retrieval and restoration of archived information in the event of a disaster, equipment failure, and/or accidental loss of files.

The goals of this backup policy will be as follows:

- to safeguard the information assets of the University,
- to prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster,
- to permit timely restoration of information and business processes should such events occur, and
- to manage and secure backup & restoration processes and the media employed within these processes,

Scope

The Information and Communications Technology Directorate is responsible for providing policy-based, system level, network-based backups of server systems under its stewardship. This document outlines the policies for backup implementation that define:

- Selections: what information needs to be backed up on which systems
- Priority: relative importance of information for purposes of the performing backup jobs.
- Type: the frequency and amount of information to be backed up within a set of backup jobs.
- Schedule: the schedule to be used for backup jobs.
- Duration: the maximum execution time a backup job may execute prior to its adversely affecting other processes.

• Retention Period: the time period for which backup images created during backup jobs are to be retained.

9.2.1.1. Backup Creation

9.2.1.2. The Information and Communications Technology Directorate will maintain the following type of backup profiles:

9.2.1. Policies

Backups will be created using industry standard data backup software that support "enterprise lev-el" data assurance. The product, defined by the data backup standard, must support scheduled backups, full or differential or incremental backups, and centralized management.

Standard Backup: The standard backup is provided for most centralized University computer systems. The backup could be full, differential, or incremental. The frequency of backup could be daily, weekly, or monthly and is dependent upon the application. The retention of these backups could vary from 1 week up to 2 months.

Critical System Backup: Certain enterprise-wide systems are deemed critical to University operations and dictate longer retention periods from 6 months up to 1 year. The type, frequency and retention period are different for different applications. Prior to a major upgrade of a production system, database, or application, a full system backup is performed and retained for 6 months.

Special Request Backup: Some departments or applications may require an exception to the standard backup retention periods mentioned above. Exceptions are permitted, but must be fully documented

No Backup: ICT Directorate' is responsible for backing up data that is stored in central systems and databases. Data residing on individual workstation hard drives is the responsibility of the user to backup. Furthermore, the systems that fall under this category might include development or test systems that do not contain important business or academic data. Students, faculty, staff and third parties who store data on University

equipment are responsible for ensuring the data is stored in a way that will ensure it is properly backed up. However, most systems that are centrally managed by the ICT Services are backed up on one of the schedules listed above.

9.2.1.3. Storage Locations and Retention

o to check for and correct errors,

o to monitor duration of the backup job, and

o to optimize backup performance where possible.

1. Period of Backups

• Unless a system supporting an application or business function requires a custom retention period, the Department of ICT Services will maintain full and incremental backups. After a successful backup, data will be stored in a secure, off-site media vaulting location for an appropriate period for disaster recovery purposes.

2. Backup Verification

• On a periodic basis, logged information generated from each backup job will be reviewed for the following purposes:

• The department of ICT services will identify problems and take corrective actions to reduce any risks associated with failed backups. Test restores from backup tapes for each system will be performed. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly.

9.2.1.4. Media Management

1. Media will be clearly labeled, and logs will be maintained identifying the location and content of backup media. Backup images on assigned media will be tracked throughout the retention period defined for each image.

9.2.1.5. Storage, Access, and Security

All backup media will be stored in a secure area that is accessible only to designated university staff or employees of the contracted secure off-site media vaulting vendor used by the Department of ICT Services. Backup media will be stored in a physically secured, fireproof place when not in use. During transport or changes of media, media will not be left unattended

9.2.1.6. Retirement and Disposal of Media

`o the media no longer contains active backup images or that any active backup images have been copied to other media,

o the media's current or former contents cannot be read or recovered by an unauthorized party.

9.2.1.7. Disaster Recovery Considerations

1. As soon as is practical and safe post-disaster, the ICT Directorate' will:

1. Prior to retirement and disposal, the ICT Directorate' will ensure the following:

o restore existing systems to working order or obtain comparable systems in support of defined business processes and application software,

o Restore the backup system according to documented configuration so as to restore server systems,

o Obtain all necessary backup media to restore server computing systems, and

o Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery in the Disaster Recovery Plan.

9.2.1.8. Documentation

1. Essential documentation will be maintained for orderly and efficient data backup and restoration.

References

University of Richmond, Backup Policy, https://is.richmond.edu/policies/technology/Computer_Systems_Backup_Policy_May2017.pdf

University of Utah, Backup and Recovery Policy, https://it.utah.edu/policies/UITDataBackupandRecoveryPolicy.pdf

Penn State University, Data Backup and Retention Procedure, https://newkensington.psu.edu/sites/default/files/pdf/psu-nk-its-012data_backup_and_retention.pdf

9.3. Password Policy

This policy describes the University's requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking

programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the policy statement found below.

Scope

This policy applies to anyone accessing or utilizing the University's network or data. This use may include, but is not limited to, the following: personal computers, laptops, mobile phones, and hand-held factor computing devices (e.g., PDAs, USB memory keys, and electronic organizers), systems and servers. This policy covers departmental resources as well as resources managed centrally.

9.3.1. Policies

9.3.1.1. Individuals must have a unique identifier and password for each University account.

9.3.1.2. All university owned electronic devices that access confidential/restricted University data must have password protection enabled.

9.3.1.3. Passwords must be stored in irreversible encryption format whenever possible.

9.3.1.4. Passwords must contain at least eight (8) characters, in combination of the following:

1. At least one upper case alphabetic character.
2. At least one lower case alphabetic character.
3. At least one numeric character (1, 2, 3, etc.).
4. At least one punctuation or symbol character (@, $, #, etc.).

9.3.1.5. Do not use ‘, “or blank spaces as they may not work with all University systems.

9.3.1.6. Faculty and staff passwords must be changed at least once every six months and students, emeriti and retiree passwords must be changed at least once every year. Reminders to change your password will begin at "x" number of days from expiration and continue at regular times until the password expires. All will include the link to changing your password.

9.3.1.7. Administrator user accounts that have system-level privileges granted through group memberships must have unique passwords for each account(s) held by that user.

9.3.1.8. Usernames and passwords are for the use of the individual to whom they were granted and must not be shared.

9.3.1.9. Help Desk and system administrators must verify the identity of users when assigning or resetting passwords.

9.3.1.10. All vendor supplied default passwords must be changed prior to any application or program's implementation to a production environment.

References

• University of West Michigan, Password Policy, https://wmich.edu/it/policies/password

• Brown University, Password Policy, https://it.brown.edu/computing-policies/computing-passwords-policy

• University of Richmond, Password Policy, https://is.richmond.edu/policies/technology/password-policy.html