Chhatrapati Shahu Ji Maharaj University Kanpur

(FORMERLY KANPUR UNIVERSITY, KANPUR)

Policy

for

Information Technology

Information Technology Policy

Table of Contents

Table of Contents

1. Acceptable Use of Electronic Information Resources

Purpose:

This policy establishes the guidelines for utilizing electronic information resources at CSJM University in Kanpur.

Applies to:

This policy is relevant to all departments of CSJM University, and it applies to faculty, staff, students, official university affiliates, and any other individuals who utilize either University electronic information resources or private electronic information resources for the purpose of conducting University business.

Policy Statement:

Introduction

In order to support its mission of education, research, and public service, CSJM University in Kanpur offers electronic information resources to its faculty, staff, students, official university affiliates, and other individuals. These resources include e-books, online databases, e-journals, and other digital content.

The University recognizes the importance of creating an inclusive and open academic community that values civil discourse, tolerance, and respect for all individuals. To uphold these values, the University expects that the use of electronic information resources should align with these same expectations. It is important to ensure that these resources are utilized in a responsible manner that reflects the University's commitment to promoting a diverse and inclusive environment for all members of the academic community.

Responsibilities of Users

Users of electronic information resources are expected to adhere to a set of responsibilities to ensure ethical and lawful use of the resources. These responsibilities include:

- Using electronic information resources in a manner consistent with the requirements of the University, maintaining their integrity and respecting their intended use, as well as the privacy, confidentiality, and security of the information.

- Not sharing access privileges with others or attempting to gain unauthorized access to secured information resources.
- Using University resources to conduct University business and disclosing any University-related information or records in personal or private email accounts or electronic devices if requested under the CSJMU Open Records Act or other University needs.
- Not attempting to circumvent login procedures or gain unauthorized access, which may be a crime under federal, state or local law.
- Using electronic information resources in a manner that does not interfere with, compromise, or harm the performance, functionality, or integrity of the University's electronic information resources, including adherence to University standards regarding software updates and protections, data handling, and other policies and procedures.
- Respecting network capacity as a shared resource and not performing operations that degrade network performance for other users, including not engaging in activities that infringe on the rights and/or productivity of other users.
- Respecting the rights of copyright owners and obtaining permission from owners before using or copying protected material, including music, movies, software, documents, images, or multimedia objects, and not engaging in systematic or excessive downloading or printing of content.
- Using electronic information resources for incidental personal use as long as it does not interfere with University operations, violate University or Regents policies, create an inappropriate atmosphere for employees, generate incremental identifiable costs to the University, and/or negatively impact the user's job performance.
- Obtaining written approval before using University resources for external activities, with permission granted only when it further the mission of the institution, and making arrangements for reimbursement of the University for Institutional Materials, facilities, or services used in the external activity.
- Not using electronic information resources for commercial purposes, personal financial gain, or to solicit support for outside organizations not authorized to use University facilities.
- Using electronic resources to exchange ideas and opinions, including political issues, but not using University electronic resources to support partisan political candidates, party fundraising, or causes.
- Not representing oneself as someone else without previous written authorization.
- Not engaging in any conduct not protected by the First Amendment, including true threats, incitement to imminent violence, fighting words, and unlawful, targeted harassment, or deliberately destructive behaviour.

Responsibilities of the University

The CSJM University recognizes that its electronic information resources are state-owned and therefore has the responsibility to ensure that they are used appropriately. While the

University values trust and respect among its community members and generally does not monitor individual users' routine use of electronic resources, it must still monitor these systems for misuse. As a result, the confidentiality, privacy, or security of data, email, or other information transmitted or stored on the University's electronic information resources cannot be guaranteed. If University officials suspect that a user may be violating University or Regents policies, federal, state, or local law, or engaging in activities that conflict with their University responsibilities, the system administrators may inspect and record the files of that user, including word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software.

Reporting Irresponsible Use of Electronic Information Resources

It is important for users and units to report any unauthorized access attempts or improper usage of CSJMU information resources. The Computer Incident Response Team (CIRT), led by the CSJMU System Manager, is responsible for identifying and responding to incidents, and working with departmental technical liaisons to ensure effective response time and communication.

If you observe or are informed of a security or abuse problem with any University information resource, including violations of this policy, it is important to report it to the authorities. The CIRT is responsible for coordinating evidence gathering and documentation, and seeking advice from representatives from the Vice-Chancellor and Vice Chancellor's Office, and others as required by the particular incident.

Any apparent violations of IT policy will be reported to the Vice-Chancellor for disposition according to standard procedures and University policies on violation of policy. It is important for all users and units to understand their responsibilities and obligations regarding the use of CSJMU information resources to maintain a secure and trustworthy computing environment.

Freedom of Expression Acknowledgment

This statement emphasizes that the policies and rules mentioned in the preceding sections of this document are not intended to violate any Indian laws or regulations regarding freedom of speech or expression. The policy also ensures that it does not discourage individuals from hearing diverse perspectives and opinions, as long as they are within the confines of the law. Additionally, any regulation or restriction of protected speech or expression will be content-neutral and limited to narrowly drawn time, place, and manner restrictions consistent with the Indian Constitution's principles. The policy seeks to strike a balance between maintaining the University's intellectual environment and protecting individuals' freedom of expression.

2. Electronic Mail Policy

Purpose:

To define appropriate use of electronic mail in the University.

Applies to:

This policy applies to faculty, staff, students, official university affiliates, and any other individuals who use University electronic mail.

Policy Statement:

CSJMU provides electronic mail services to its students, faculty, staff, and affiliates for activities relating to instruction, research, clinical and public service, management, and administrative support. Incidental personal use is also permitted as long as it does not interfere with CSJMU operations, generate incremental costs, or negatively impact job performance. However, CSJMU email cannot be used for commercial purposes, personal financial gain, distributing chain mail, or supporting outside organizations without written approval from the Vice-Chancellor or Vice-Chancellor nominee. Political use of CSJMU email is also prohibited.

While the University does not routinely monitor or screen email, complete confidentiality or privacy cannot be guaranteed due to the nature of the medium and the University's accountability as a public institution. The Vice-Chancellor or Vice-Chancellor nominee may authorize access to employee or student email in situations involving health or safety, possible violations of University codes or policies, possible violations of laws, legal responsibilities or obligations of the University, or the need to locate information required for University business.

It is the responsibility of faculty, staff, and students to ensure that their email address on file with the University is accurate and up-to-date. If a faculty or staff member changes his or her email address, the individual must update his or her contact information in the University directory. If a student changes his or her email address, he or she must update his or her contact information through the Office of the Registrar.

The University is not responsible for delays or failures in the delivery of email communications due to technical problems or failures outside of its control. Users should take appropriate measures to protect the confidentiality, integrity, and availability of their email accounts and the information contained therein. This includes taking appropriate

measures to protect their account passwords, not sharing passwords with others, and using encryption when necessary.

The CSJMU email system can be utilized for surveying students, faculty, and staff members. If someone wishes to conduct surveys through email, they should contact the Office of the Vice-Chancellor for approval. It's essential to note that CSJMU email accounts are owned by the University, and they will be deactivated upon graduation or separation from the institution.

3. Password Policy

Purpose:

This policy aims to set a benchmark for generating robust passwords, safeguarding those passwords, and establishing guidelines for the frequency of password updates.

Applies to:

The scope of this policy includes:

1. All personnel who are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CSJMU facility;
2. All individuals who have access to the CSJM University network; and
3. All systems that store any non-public CSJMU information.

Policy Statement:

Passwords play a crucial role in computer security, serving as a crucial defence mechanism against unauthorized access to electronic resources. They aid the University in controlling inappropriate or unauthorized access to various network resources such as user-level accounts, web accounts, email accounts, screen saver protection, and local router logins. It is vital to note that a poorly selected password may lead to the compromise of University data, systems, or the network. As a result, all CSJMU students, faculty, and staff have a responsibility to adhere to the guidelines provided below to select strong passwords and protect them. Contractors and vendors with access to University systems must also comply with these requirements.

Creation of Passwords

Users of University systems must adhere to the following standards when creating passwords, where technology allows:

- Your password must be 8 to 32 characters long and must contain:
- At least one special character (&,#,-,_, etc.)
- At least one uppercase letter
- At least one lowercase letter
- At least one digit (0-9)

These provisions shall be enforced electronically whenever possible.

Protecting a Password

- Passwords must be treated as confidential information.
- Passwords must not be included in email messages or other forms of electronic communication.

Sharing a Password

- CSJMU Online IDs are issued to individuals for their exclusive use, and passwords may not be shared.
- Departmental account passwords must be shared only with appropriately designated departmental personnel.
- Users need to beware of "phishing" or other social engineering scams where a user may have a password requested over the phone. University information technology personnel (i.e., Computer Center, Departmental Technical Staff), as a best practice, do not request a user's password over the phone.

Reporting a Password Compromise

- Suspected compromises of passwords must be reported immediately to the CSJMU Computer Center.
- The password in question must be changed immediately.

Consequences:

Failure by faculty, staff, and student employees to comply with this University policy may result in disciplinary action for misconduct and/or performance, following the appropriate administrative process related to their employment. In the case of students, violations of this policy may result in non-academic misconduct proceedings based on their status as a student. Any individuals, including faculty, staff, student employees, and students, found to be in violation of this policy may also be subjected to the suspension of particular information technology services.

4. Data Center and Server Room Policy

Purpose:

The objective of this Policy is to establish the essential criteria for creating, deploying, safeguarding, supervising, maintaining, securing, and decommissioning a server room or data centre at CSJM University in Kanpur. It pertains to all employees (including faculty and staff), students of CSJM University, Kanpur, and other individuals covered by the policy (such as vendors and independent contractors) who use University technology resources while conducting University business.

List of Equipments available in the Data Centre:

The data centre is established at the ground floor of the Computer Center of the University. The room is having Genset power backup and UPS backup (180 minutes).

Smart Rack:

All the equipments of data center are kept in a smart rack (Make: RITTAL) of size 2x42U. This rack is equipped with an automatic firefighting system, access control system (i.e. only authorized users through biometric authentication can access the system) and a redundant cooling system. The equipments installed in the rack are as follows:

Firewall:

The data center is protected through firewall system (Sophos XGS 5500 with 03 Years Xstream Protection) to prevent external threats and attacks. This firewall is also used for the safety of campus network.

Switches:

Name of Switch	Make	Model	Qty
SAN Switch 12 Ports	CISCO	DSC9148S-12PK9	1
IP Based KVM Switch with LCD Console	ATEN	CL5716I	1
Layer-3 Core Switch 48 Ports	CISCO	CISCO-L3C-C9500-48Y4CA	2
Layer-3 Distribution Switch 48 Ports	CISCO	CISCO-L3D-C9500-48Y4CA	2
Layer 3 – Access Switch 24 Ports	CISCO	CISCO-L3A-C9300-24UXBA	1

Servers:

Name	Make	Model	Qty
High Compute Server **2xAMD, CISC(X86), 32 Core, 256 GB RAM**	DELL	DELL EMC PowerEdge R6525	4
High Performance Server **2xAMD, CISC(X86), 16 Core, 512 GB RAM**	DELL	DELL EMC PowerEdge R6525	2

Further, the data center have 192 cores windows server licences (paper) and 3 RadHat Enterprise Edition Licences.

Unified Storage:

The data center is equipped with a unified storage system (make DELL EMC) with 200TB of usable space.

Endpoint Detection and Response (EDR) Software:

The data center is equipped with Central Intercept X Advanced for Server (10 Licenses) with EDR for the protection of servers.

Data Classification and Handling Procedures:

A. Determine How Much Protection your Information Needs

The degree and form of protection to be implemented for your data are determined by an evaluation of the necessity for confidentiality and/or the criticality of the information. The following table provides an overview of this procedure.

How would you describe your information?

Is it Confidential? Is there a high need for Integrity? Is there a high need for Availability?	Level I Protection	**STOP!** **SPECIAL CARE IS REQUIRED**
Is it Sensitive? Is there a medium need for Integrity? Is there a medium need for Availability?	Level II Protection	**BE VERY CAUTIOUS**
Is it Public? Is there a low need for Integrity? Is there a low need for Availability?	Level III Protection	**PROCEED WITH AWARENESS**

Level I – **Confidential Information:** High risk of significant financial loss, legal liability, public distrust or harm if this data is disclosed. Examples include:

1. Health information
2. Student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.
3. Financial information

4. Credit or payment card standards
5. Passwords and PINs
6. Personally Identifiable Information
7. Personnel data
8. Individually identifiable information created and collected by research projects
9. Certain research data with National Security implications
10. Data subject to protection pursuant to non-disclosure agreements
11. Audit working papers
12. Email covering topics listed above

Level II – **Sensitive Information:** Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, and public distrust, or harm if this data is disclosed. Examples include: Audit reports

1. Email addresses that are not a public record
2. Other grants and contracts (not included above)
3. System security information such as firewall rules and hardening procedures

Level III – **Public Information:** Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust or harm if this data is disclosed. Examples include:

1. University directory information
2. Blogs
3. Web pages
4. Course offerings
5. Annual reports, etc.

B. Collect Only What is Necessary

	Level I	Level II	Level III
A. Collect only the minimum required amount of data to fulfill institutional responsibilities.	Required	Required	Required
B. Collect Social Security Numbers only as required to achieve necessary institutional purpose.	Required	Not Applicable	Not Applicable
C. Retain full credit card numbers (electronically or on paper), only if written approval has been obtained from Finance Officer.	Required	Not Applicable	Not Applicable

C. Provide Minimum Necessary Access

	Level I	Level II	Level III
A. Limit access to information to those with a legitimate interest ("need to know" or "need to do") based on their institutional responsibilities.	Required	Required	Required
B. Access or attempt to access only information required to fulfill your institutional responsibilities.	Required	Required	Required
C. DO NOT log in for other people who are trying to access the computer system, e-mail system or other device. Never use anyone else's login information.	Required	Required	Required
D. Grant access only to those authorized by the data owner.	Required	Required	Recommended
E. Use an authentication process to control access to non-public file systems. • Authentication means individuals attempting to gain access must have been previously approved for access and must prove their identity for each requested access by entering their user name and password or using another approved method of identification.	Required	Required	Not Applicable
F. Ensure all vendor access has been approved by the IT Security Office.	Required	Required	Required
G. Track and review who has gained access by recording ALL access in a system log. At a minimum, successful and failed login events, successful and failed account management events, and successful and failed policy and system events should be logged. (The logs should be stored in a way that precludes system administrators from altering/deleting them. The logs will be reviewed for anomalies monthly.)	Required	Recommended	Recommended
H. Information must be protected from unintended access by unauthorized users. • Guard against unauthorized viewing of such information displayed on your computer screen, keyboard, or login screen. • Do not leave information unattended and accessible. • Do not leave keys or access badges for rooms or file cabinets containing information in areas accessible to unauthorized personnel. • When printing, photocopying or faxing information, ensure that only authorized personnel will be able to see the output. If these machines retain the last document or several documents in memory, be sure to clear the memory after sensitive documents	Required	Required	Recommended

have been processed. Use a fax cover sheet with a confidentiality statement.			
I. Respect the confidentiality and privacy of individuals whose records are accessed by observing ethical restrictions that apply to the information accessed and by abiding by all applicable laws and policies with respect to accessing, using, or disclosing information. At a minimum: • Ensure Confidentiality Agreements are signed by staff with access to those systems storing and/or processing Sensitive Information. • Use an approved login banner on services that support it in order to inform users of their rights and responsibilities.	Required	Required	Required
J. Revoke or modify access rights and privileges to information for any individual with new or different responsibilities. • This may include obtaining keys, deactivating user accounts, changing the level of network access, changing codes for key punch systems, or deactivating passwords used to obtain access.	Required	Required	Not Applicable
K. Establish a periodic review (at a minimum quarterly) of user accounts including the related access rights and privileges for employees in your unit and modify those rights when appropriate. • Maintaining a current list of employees and their corresponding access rights is one way to facilitate the review process.	Required	Required	Not Applicable
L. Restrict servers to a single primary function.	Required	Recommended	Recommended
M. Disable or remove unused services, applications, ports, and user accounts.	Required	Recommended	Recommended
N. Physically secure access to operating systems, servers, and network equipment by placing them in areas that allow access to be restricted.	Required	Required	Recommended
O. Secure portable devices and portable media devices when unattended (e.g., laptop, PDA, smartphone, etc., and CD's, DVD's, floppy disks, USB/Flash/Thumb drives, etc.).	Required	Required	Recommended
P. Secure backup media from unauthorized physical access.	Required	Required	Recommended
Q. Ensure system setup is done in an environment that is only accessible to authorized administrators.	Required	Required	Recommended
R. All systems shall use only the below CSJMU-approved network and system login banner: "Access to electronic resources at the University of CSJMU is restricted to employees, students, or individuals authorized by the University or its affiliates. Use of this system is subject to all policies and procedures set	Required	Required	Recommended

forth by the University. Unauthorized use is prohibited and may result in administrative or legal action. The University may monitor the use of this system for purposes related to security management, system operations, and intellectual property compliance."

D. Disclose Only the Minimum Necessary Information

	Level I	Level II	Level III
A. Do not discuss or display information in an environment where it may be viewed or overheard by unauthorized individuals.	Required	Required	Recommended
B. Limit a disclosure to the amount of information reasonably necessary to achieve the purpose of the disclosure.	Required	Required	Required
C. Disclose information only when necessary and only to the extent that such disclosure is consistent with University policy and permitted or required by law.	Required	Required	Recommended
D. Ensure the Office of the General Counsel reviews all subpoenas, search warrants, or other court orders prior to release of information.	Required	Required	Required
E. Refer requests for information from media representatives (i.e., reporters, TV news crews, etc.) to the Office of University Relations.	Required	Required	Required
F. Report immediately any potential or suspected breach or compromise of, or unauthorized / unexplained access to University information (electronic or paper) to the system manager.	Required	Required	Required

E. Safeguard Information in Transit

	Level I	Level II	Level III
A. Use secure methods of transmission when sending any Private, Confidential, or Sensitive data. • Secure methods include, but are not limited to: ○ Encryption (i.e., at least Triple DES or AES; use AES-256 when possible), ○ Virtual private network (VPN), ○ Secure Shell (HTTPS), ○ Secure FTP (SFTP), ○ Encrypted and password protected CDs separated from passwords (phoned in) and/or the decryption keys (hand carried), ○ Facsimile transmission to secure faxes, etc.	Required	Required	Recommended
B. Encrypt email when sending Private, Confidential, or Sensitive information, even to other authorized users. The encryption method and key storage method must be approved by IT Security. • Examples of information that should not be sent by email (unless encrypted) include, but are not limited to: ○ Student lists, ○ Data subject to the Health Insurance Portability and Accountability Act (HIPAA), ○ Data subject to the Gramm-Leach Bliley Act (GLBA), or • Use a confidentiality statement at the beginning or end of e-mails to notify the recipient of confidential content.	Required	Required	Recommended
C. Send faxes only when the intended recipient is present. • Use a confidentiality statement at the beginning or end of e-mails to notify the recipient of confidential content. • Verify fax numbers prior to transmission.	Required	Required	Recommended
D. Ensure information (including device(s) containing information) is physically secure at all times when carrying or hand-delivering it to a new location.	Required	Required	Recommended
E. Remove information from secure locations only with prior approval.	Required	Required	Recommended
F. Access information remotely using only secure methods approved by the CSJMU IT Security Office.	Required	Required	Recommended
G. Accessing or transferring Private Information (Confidential or Sensitive information) using on-campus wireless connections is NEVER	Required	Required	Not Applicable

appropriate, unless the wireless network is encrypted and it has been approved by the CSJMU.			
H. Accessing and transporting Social Security Numbers via a portable device is NOT appropriate.	Required	Not Applicable	Not Applicable

F. Secure Physical Equipment and Resources

	Level I	Level II	Level III
A. Actively "lock" your workstation when you are away from your desk; do not just wait for the screen saver feature to self-activate.	Required	Strongly Recommended	Strongly Recommended
B. Use "strong" passwords that are not easily guessed. Ensure that computer monitors are situated in a manner that login screens cannot be observed by passers-by. Any passwords written down should be securely stored.	Required	Required	Required
C. Place devices that can be used to print information in secure locations.	Required	Required	Recommended
D. Use a variety of methods to help prevent information compromise. • Use a properly configured and currently patched firewall. • Actively monitor systems using Anti-virus software that is updated daily. • Actively monitor systems using Anti-spyware that is updated daily. • Obtain automatic security updates, and implement them expediently. • Click "No" if your web browser offers to save passwords. Alternatively, turn off the password saving feature in the browser. • Be aware of the risks to privacy of information when using desktop search features like Google Desktop Search.	Required	Required	Required
E. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive, or laptop. • Select portable device models that provide security options to protect information stored on the drive. • For example, Personal Data Assistants (PDAs) may be set to require a password when turned on or are inactive for a few minutes. • Enable pass-codes and inactivity timers on mobile devices that support them.	Required	Required	Recommended

• Employ whole disk encryption on mobile computers (where the encryption method and key strength level are approved by IT Security).			
F. When evaluating new software or appliances, request a security review of the proposed items by the IT Security Office BEFORE purchasing or installing. • The request to ITSO should be in writing, signed by the purchasing authority, prior to final selection of vendors or products.	Required	Strongly Recommended	Strongly Recommended
G. When making a change to a service, system, or business process, consider whether any currently functioning security measures will be disrupted. All changes or modifications to the standard architecture shall be documented along with any justifications.	Required	Required	Recommended
H. Conduct regular system backups. Backups help ensure the availability of data necessary to fulfill University responsibilities in the case of device failure, disaster or theft. • Restoration from backup should be regularly verified. • Security logs in addition to primary data should be backed up. • Backup files should be stored at a secure location sufficiently apart from the primary data source/storage so as not to be impacted by an event that might render the original data unusable.	Required	Strongly Recommended	Strongly Recommended
I. Immediately contact the local area public safety department if there is a theft of any computer, electronic storage media, portable or personal device containing or that has been used to process University information. • Also alert the department responsible for the device. • If you suspect any Private Information was on the stolen device, contact the Information Technology Customer Service Center (785-864-8080). The Information Technology Customer Service Center will notify the CSJMU Privacy Officer and/or the CSJMU IT Security Officer as required by the particular incident.	Required	Required	Required

G. Safeguard Information in Storage

	Level I	Level II	Level III
A. Employ physical protection for all devices (electronic and non-electronic) used to store data.	Required	Required	Recommended

• Limit physical access, including the ability of the public to inadvertently view the data (i.e., as passersby). • Filing cabinets & drawers, offices, labs, and suite doors containing data must be locked. Do not leave data on unattended desk tops or leave file drawers unattended and unlocked. • When not in use, all easily transportable devices should be secured (e.g., in locked cabinets or drawers). • Users of lap-top and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the University. • Electronic media used to store Confidential Information must be secured by password-protected encryption. The encryption method and key strength level must be approved by IT Security. • Encrypt Confidential Information stored on any portable device (laptop, PDA, smartphone, etc.) or other portable media device (CD's, DVD's, floppy disks, USB/Flash/Thumb drives, etc.) and utilize available security features on the device. The encryption method and key strength level must be approved by IT Security.			
B. Store Confidential or Sensitive Information in a separate location when possible.	Required	Required	Not Applicable
C. Always encrypt Confidential and Sensitive Information prior to storage. Encrypting data helps ensure that if an access control is bypassed, the information is still not readily available. A standard and published encryption standard should be used. The encryption method and key strength level must be approved by IT Security. • Encrypt media stored off-site or have a documented process to prevent unauthorized access.	Required	Required	Recommended
D. Securely store information. • Limit custody/access to as few people as possible to enhance accountability. • Document transfers of custody.	Required	Required	Recommended
E. Store data on systems that support access control (as described in Section 3 of this policy).	Required	Required	Recommended
F. Retain Social Security numbers only when required (by a "business-related" purpose) and ONLY in an encrypted file or truncated to last 4 digits. • The following identification mechanisms should also be handled and protected with care: 1. CSJMU Student ID numbers, 2. CSJMU Employee ID numbers, 3. State of CSJMU Employee ID numbers, and 4. the CSJMU Online ID.	Required	Not Applicable	Not Applicable

H. Dispose of Information Securely When No Longer Needed

	Level I	Level II	Level III
A. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction. • No records that are currently involved in, or have open investigations or audits, or records for which a litigation "hold" has been issued, shall be destroyed or otherwise discarded.	Required	Required	Required
B. Review, purge and shred printed documents regularly (in accordance with published destruction schedules). • Shred documents prior to disposal/recycling. • Adequately secure any documents that must be stored temporarily prior to shredding so they are not accessible to anyone without authorization.	Required	Required	Not Applicable

Virtual Private Network (VPN) Remote Access Procedure:

- Requests for VPN Remote Access Service by users must be submitted through their departmental IT Technical Liaison or designated system administrator. VPN access is limited to faculty and staff.
- Each department determines which individuals will be granted authorization for VPN Remote Access Service within their department.
- VPN Remote Access Service is only authorized after confirmation by the IT Liaison or designated system administrator.
- Information Technology provides support for the VPN network device, the VPN client, a method for Systems Administrators to grant their users access to the VPN service through the DCDR registration process, documentation for installing the VPN client, and 24x7 system support.
- The departmental IT Technical Liaisons or designated system administrators are responsible for assisting users with the installation of the VPN client and resolving any issues related to individual user client set-up and operation.

5. Learning Management Systems (LMS) Policy

Purpose:

To provide decision-making guidance for the use of learning management systems (LMS) ***GyanSanchay*** developed by CSJM University, Kanpur

Policy Statement:

A. Access

Access to LMS software, materials, and affiliated online tools will be granted as follows:

a) Each CSJMU faculty, staff, and student is provided with a single account on the Gyansanchay LMS for all their activities. Users can access various course-independent features, such as calendar, task, and organization sites, using their CSJMU Online ID (username and password).

b) To obtain full access to the LMS, students must be enrolled in courses that have been made available by their instructors. Instructors have the option to grant partial access to currently enrolled CSJMU students who are in the process of adding a course to their schedule.

c) The access to course sites is typically available to students until the end of a term, after which instructors may make the course unavailable. Allowing access beyond the usual cut-off will not be encouraged to prevent possible confusion and copyright issues.

B. Course Management

Pages on the LMS server are managed with the goals of reducing faculty time and effort needed to utilize online tools and materials, and improving server performance by eliminating redundant or unnecessary demands on the database.

a) All course sites are kept on the LMS server, regardless of whether they are actively used by students or not, to provide continuous access to instructors throughout the year.
b) While there is no official limitation on the size of course sites, courses generated in the LMS have a default quota of 2000MB. If a course site is using a large amount of storage, Educational Technologists will work with faculty to help them compress files or move materials to another environment to use space as efficiently as possible.

c) Instructors are encouraged to copy forward materials from previous semester course sites instead of using one site in multiple academic terms.
d) Instructors may transfer course sites and materials to another faculty member or give access to their course site. However, a course site will not be reassigned to a new instructor for reuse without written permission from the original instructor, department chair, program director, or college dean. If a faculty member leaves CSJMU for other employment, they may request a copy of their course site(s) to take along or request that a copy be transferred electronically to the new institution.

C. Copyright Issues

Faculty are required to respect the property of others by obeying copyright law and requesting permission, when appropriate, before using the work of others.

a. ***Posting Copyrighted Materials*** - Copyright law and Fair Use Guidelines allow faculty to provide access to copyrighted materials using the LMS system.
b. ***Linking to External Sites from the LMS***- Linking to external websites from the LMS is a good practice as it allows instructors to provide access to a wide range of materials without violating copyright laws. It also ensures that the materials remain in their original environment and are not altered in any way. Instructors should make sure that the links are functional and up-to-date, as broken links can frustrate students and impede their learning. They should also periodically check the links to ensure that they lead to appropriate and relevant content. By linking to external websites, instructors can provide a rich and diverse learning experience for their students while avoiding legal and ethical issues related to copyright infringement.

6. Network Policy

Purpose:

To define the University network and establish operational provisions governing use and operation of the network.

Applies to:

This policy applies to all users directly or virtually connected to the University network

Policy Statement:

Principles

To ensure the security of the network, the University has established policies and procedures to govern the use of the network. These policies include guidelines for the use of network resources, access controls, security protocols, and monitoring of network activity. All users of the University network are required to abide by these policies and to take appropriate measures to protect the security of the network and the information that is transported over it.

In order to maintain the reliability and efficiency of the network, the University has established standards for the installation and maintenance of network infrastructure, as well as for the use of network resources. These standards are designed to ensure that the network is able to meet the needs of all users, while minimizing downtime and other disruptions to service.

Finally, the University network is designed to be scalable, so that it can be expanded or upgraded as needed to meet the changing needs of the University community. This scalability is achieved through the use of modular, standardized components and the implementation of best practices for network design and management. By adopting these standards and best practices, the University is able to provide a reliable, secure, and efficient network infrastructure that is able to meet the needs of the entire University community.

General Policy Provisions

These are policies and guidelines related to the management and use of the University network. The policies are designed to ensure the safety, security, and reliability of the

network, as well as compliance with applicable security policies, procedures, and practices.

- The IT department is responsible for managing and administering the University network, determining technical specifications, and establishing standards for devices connected to the network. Devices connecting to the University network must comply with applicable security policies and must be centrally registered, and the Network team will review devices on a regular basis for the latest security patches and anti-virus software.
- Users connecting to the University data network through the CSJMU VPN must use the centrally-provided service and comply with the CSJMU VPN Policy, and other VPN services are not allowed. The IT Security Office may utilize additional VPN services to enforce confidentiality and integrity of campus data and assets.
- Units or users are not allowed to attempt to implement their own network infrastructure or extend the University network without permission from Information Technology. Devices connecting to the University's data network must use the central Dynamic Host Control Protocol server and the central Domain Name Service (DNS). Units are responsible for expenses associated with unauthorized installation, modification, or resulting repair.

7. Firewall Policy

Purpose

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and the internet or other external networks to prevent unauthorized access, hacking, or data breaches. However, a firewall cannot prevent malicious or illegal activities from within the network, such as insider threats or malware introduced by an authorized user. Therefore, it is important to have a comprehensive security policy that includes other measures such as access controls, user education, antivirus software, and regular security audits.

The purpose of this policy is to provide comprehensive guidance on the design, installation, security, monitoring, maintenance, protection, and decommissioning of a data centre or server room at CSJM University in Kanpur. It is applicable to all individuals who have access to and use University technology resources for conducting University business, including employees (faculty and staff), students, vendors, independent contractors, and other relevant parties.

Scope

This policy is applicable to all users of the CSJM University network, including faculty, staff, administrators, contractors, students, systems, applications, and networks.

Definitions

Firewall

A firewall is a device, both hardware and software-based, that regulates access between two separate networks. There are various methods for implementing this access control, but the primary objective of a firewall is to enforce a network security policy.

Firewall System

In a firewall system, there are additional controls beyond the base firewall product, which may or may not be included. These additional controls can include solutions for content blocking or filtering, such as anti-virus email gateways, intrusion detection systems, audit and logging tools, mobile code monitors (for ActiveX and Java), integrity checkers, email content scanners, and URL blockers.

Responsibilities

The implementation and maintenance of the University's network perimeter firewall is the responsibility of the Network Security Services (NSS). As such, NSS is also accountable for activities associated with this policy. However, on a daily basis, all employees are responsible for information systems security. While specific guidance and direction for information systems security fall under the purview of NSS.

Policy and Procedures

The Firewall permits the following for outbound and inbound Internet traffic:

• **Outbound**- Allow ALL Internet traffic to hosts and services outside of CSJM University with the exception of known security vulnerabilities. This allows anyone connected to the CSJM University Network to utilize all services on the Internet with the exception of known vulnerabilities.

• **Inbound**- Only specific services which support CSJM University mission will be allowed to be accessed from the Internet. The chart below identifies the most common services used for Internet communications within the CSJM University environment.

Operational Procedures

Only firewall system administrators are permitted to logon to the firewall.

- Access to firewall hosts should be tightly controlled, and only firewall system administrators should have user accounts on these hosts.
- Firewall system administrators must use personal accounts and are not allowed to use group logins.
- Remote root access directly is not permitted. All root access must be through personalized logins. Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware, or configuration.
- Changes should be made based on a recorded request using the Firewall Change Request Form. However, in case of emergency modifications, personnel can request changes through phone, followed by an email and change request.
- Implementation of changes should only be carried out by authorized personnel, and an audit log must be maintained.

Changes to the CSJM University firewall can only be requested by authorized departmental technical contacts. Such requests must be made in writing or electronically, with a rationale for the change, and submitted using the Firewall Change Request Form.

Configuration

The firewall will be configured to deny any service unless it is expressly permitted.

- If no rules are defined for a University network address, traffic to or from that address must be denied.
- Access to the University network must be blocked during the firewall's start-up procedure. The firewall Operating System must be configured for maximum security.
- The underlying operating systems of firewall hosts must be configured for maximum security, including disabling any unused services.
- The firewall product suite must reside on dedicated hardware.
- Applications that may interfere with the security and effectiveness of the firewall products must not run on the host machine. The initial build and configuration of the firewall must be fully documented, providing a baseline description of the firewall system to which all subsequent changes can be applied, enabling tracking of all changes to maintain a consistent and known state.
- Security must not be compromised by the failure of any firewall component.
- If any component of the firewall fails, the default response will be to immediately prevent any further access, both outbound and inbound.
- A firewall component refers to any hardware or software that is an integral part of the firewall system. Hardware failure occurs when equipment malfunctions or is switched off. Software failure can occur due to reasons such as improper maintenance of the rules database on the firewall or incorrect installation or upgrade of software.
- IP forwarding at the operating system level must be disabled until the firewall software is operational and IP filtering policies are active.

8. Systems Development Life Cycle (SDLC) Policy

Purpose:

The objective of the Systems Development Life Cycle (SDLC) Policy is to establish the standards and procedures for creating and integrating new software and systems at CSJM University. The policy aims to ensure that all development work adheres to the relevant regulatory guidelines and standards.

Applies to:

This policy applies to all individuals who conduct software or systems development work under the auspices of the university, including employees (faculty, staff, and student employees), as well as other covered individuals such as University affiliates, vendors, and independent contractors.

Policy Statement:

The Systems Development Life Cycle (SDLC) Policy at CSJM University requires that all systems and software development work adhere to industry best practices with regard to a SDLC. The policy outlines the minimum required phases and tasks, as well as recommended steps, for system and software development. These requirements and recommendations apply to all individuals who perform any type of software or systems development work under the auspices of the University, including employees, students, affiliates, vendors, and independent contractors. Additionally, if the system or software development deals with Level 1 data in any way, then all sub-tasks and considerations listed in the respective development phases are mandatory.

A. System Initiation:

- A need or opportunity is defined.
- Concept proposal is made.
- An initial feasibility study is conducted.
- A project charter (if necessary) is formulated.

B. System Requirements Analysis:

- Analyse user needs and develop user requirements.
- Create a detailed Functional Requirements Document.

- Break down the system, process, or problem into discrete units or modules and utilize diagrams and other visual tools in order to analyse the situation or need.
- Any security requirements must be defined.

C. System Design

- This phase transforms the requirements into a Design Document.
- The functions and operations of the system or software being designed are described in detail.
- A risk analysis should be done between the System Requirements and System Design phases.
- A final design review should be done to ensure the design addresses practicality, efficiency, cost, flexibility, and security.

D. System Construction (Procurement):

- This phase entails the transformation of the detailed design documents into a finished product or solution.
- Manual and automated testing at a unit or module level is done throughout this phase by the system or software developers. Security considerations are taken into account during testing.
- A third-party product may be utilized as a system or software solution if it best fits the user requirements and is more practical from a budgetary and/or resource perspective. However, all of the next phases should be followed regardless of whether the solution was developed in-house or purchased.

E. System Testing and Acceptance:

- This phase is commonly known as the Testing phase. Its purpose is to ensure that the developed system or software meets all functional requirements as captured during the System Requirements Analysis phase. The following sub-tasks and considerations are mandatory if the system or software development deals with Level 1 data in any way:
- Representatives separate from the development group should conduct internal Quality Assurance (QA) testing to ensure that the software is functioning as expected and that there are no defects or errors.
- Representative(s) from the user group should conduct user acceptance testing to ensure that the software meets their needs and that they are satisfied with the end product.
- Documentation during testing should detail and match testing criteria to specific requirements.
- Holistic testing of the finished product should be done, which includes the final acceptance testing by the user(s).

- Final security assessment testing should be conducted to ensure that the software is secure and meets all necessary security requirements.
- Any problems identified during the previous phases must be resolved or remediated before implementation to ensure that the software is functioning as expected and meets all necessary requirements.

F. System Implementation:

- Once the finished, tested, and user-accepted system or software is ready for production, it is moved from the testing environment to the production environment.
- All development or testing tools, code, or access mechanisms must be removed from the software that is being moved into the production environment.
- Before or during this phase, any necessary user training should be provided to ensure users are able to properly use the new system or software.
- A final security assessment should be conducted to ensure the system or software is secure before it is released into the production environment.
- Once the system or software is in production, ongoing maintenance and monitoring should be conducted to ensure it continues to meet the needs of the users and remains secure. Any issues or incidents should be promptly addressed and remediated.

G. System Maintenance

- Regular maintenance and updates are performed on the system or software to ensure it remains up-to-date and secure.
- Any discovered vulnerabilities or security issues are promptly addressed and remediated.
- Any changes or updates made to the system or software should be documented and tracked.
- Periodic reviews of the system or software are conducted to ensure it continues to meet the needs and requirements of the organization.
- When the system or software is no longer needed, it is decommissioned in a secure and responsible manner, following appropriate data disposal procedures

REGISTRAR
Chhatrapati Shahu Ji Maharaj University,
Kanpur