जम्मू केंद्रीय विश्वविद्यालय

Central University of Jammu

राया-सूचानी (बागला), जिला सांबा -181143, जम्मू (जम्मू एवं कश्मीर)

Rahya-Suchani (Bagla), District Samba – 181143, Jammu (J&K)

CYBER CRISIS MANAGEMENT PLAN (CCMP)

Prepared On	09-07-2026
Prepared By	System Analyst
Reviewed By	ICT Cell Committee
Recommended By	Registrar
Approved By	Hon'ble Vice Chancellor

REVISION HISTORY

Date	Version	Description
09-07-2026	1.0	Base documentation

CONTENTS

1. INTRODUCTION & PURPOSE

The Cyber Crisis Management Plan (CCMP) establishes a strategic framework to help organizations prepare for, respond to, and initiate recovery from cyber incidents in a coordinated and effective manner.

The CCMP addresses various types of cyber crises, identifies potential targets and their impacts, defines the roles and responsibilities of key stakeholders, and facilitates coordinated cyber incident response among Central and State Government Ministries/Departments, as well as Critical Information Infrastructure organizations.

The Cyber Crisis Management Plan (CCMP) for **Central University of Jammu** establishes mechanisms to effectively manage cyber security crises, ensuring that disruptions or manipulation of critical functions, databases and services are minimized, infrequent, and controlled, thereby reducing their impact and potential damage to the organization and its employees.

2. CCMP – CONCEPT & SCOPE

The field of cyber security is rapidly evolving, with continuous technological advancements introducing new vulnerabilities and increasingly sophisticated cyber threats. As a Higher Educational Institution, the **Central University of Jammu** may be susceptible to the following cyber-attacks:

- Unauthorized access to individual systems to obtain or compromise sensitive personal information.
- Data theft or unauthorized extraction of institutional, research, or personal data.

- Attacks on web applications and online services aimed at disrupting or denying access to critical University services and resources.

3. NEED OF CCMP AT CU JAMMU

- Protection of Sensitive Information: Safeguards confidential student, faculty, staff, research, financial, and administrative data from cyber threats and unauthorized access.
- Ensuring Continuity of Academic and Administrative Services: Enables the University to maintain or quickly restore critical services such as Learning Management Systems (LMS), online admissions, examinations, ERP, email, and digital library services during cyber incidents.
- Minimizing the Impact of Cyber Incidents: Establishes a structured approach for the timely detection, response, containment, recovery, and post-incident analysis of cyber-attacks, reducing operational and reputational damage.
- Protection of Critical IT Infrastructure: Secures essential ICT assets, including servers, networks, web applications, and research computing infrastructure, against cyber threats.
- Compliance with Regulatory and Security Requirements: Supports adherence to applicable cybersecurity guidelines, data protection requirements, and directives issued by relevant government agencies and regulatory authorities.
- Enhancing Cybersecurity Awareness and Preparedness: Clearly defines the roles and responsibilities of stakeholders, promotes incident reporting, and strengthens the University's ability to respond effectively through regular training, awareness programs, and cyber security drills.

4. CYBERSECURITY THREAT LANDSCAPE

Cyber Attack	Explanation	Primary Target	Motives	Threat Actors / Elements	Common Attack Vectors
Phishing & Spear Phishing	Fraudulent emails or messages designed to trick users into revealing credentials or downloading malware.	Students, faculty, staff, administrators	Credential theft, financial fraud, malware delivery	Cybercriminals, APT groups, hacktivists	Email, SMS, fake login portals, social media
Ransomware	Encrypts files and systems, demanding payment for decryption.	Data centers, ERP, library servers, examination systems	Financial gain, operational disruption	Cybercriminal gangs	Phishing emails, malicious downloads, unpatched systems
Distributed Denial of Service (DDoS)	Floods servers or networks with traffic, making services unavailable.	University website, LMS, admission portal, ERP	Service disruption, extortion, protest	Botnets, hacktivists	Botnet traffic, compromised IoT devices
Web Application Attack (SQL Injection, XSS, CSRF)	Exploits vulnerabilities in web applications to steal or manipulate data.	Admission portals, student ERP, library systems	Data theft, unauthorized access	Cybercriminals, skilled attackers	Vulnerable web applications, insecure coding
Password Attacks (Brute Force/Credential Stuffing)	Attempts to gain access using stolen or guessed passwords.	Email accounts, VPN, ERP, cloud applications	Account compromise, privilege escalation	Cybercriminals	Automated login attempts, leaked credentials
Malicious or Negligent Insider Attack	Authorized users intentionally or unintentionally compromise systems or data.	Research data, HR records, financial information	Revenge, financial gain, negligence	Employees, students, contractors	USB devices, misuse of privileges, accidental disclosure
Cyber Espionage	Long-term targeted attacks to steal confidential information without detection.	Research laboratories, intellectual property, government-funded projects	Espionage, intellectual property theft	Nation-state actors, advanced threat groups	Spear phishing, zero-day exploits, compromised accounts

Data Breach/Data Exfiltration	Unauthorized copying or theft of confidential institutional data.	Student records, research databases, payroll, examination records	Identity theft, espionage, financial gain	Cybercriminals, insiders	Malware, compromised credentials, cloud misconfigurations
Third-Party/Vendor Compromise	Attackers exploit trusted vendors or software providers to compromise university systems.	ERP vendors, cloud services, software updates	Initial access, data theft	Organized cybercriminals, APT groups	Compromised software updates, vendor credentials
Malware/Trojan Infection	Malicious software installed to steal information or provide remote access.	Faculty laptops, student computers, laboratory systems	Data theft, botnet creation	Cybercriminals	Email attachments, pirated software, infected USB devices
Rogue Wi-Fi/Evil Twin Attack	Fake wireless networks capture user credentials and communications.	Students, visitors, faculty	Credential theft, surveillance	Cybercriminals	Fake Wi-Fi hotspots, public wireless access
Cloud Service Compromise	Exploits weak cloud security configurations or stolen credentials.	Cloud storage, Microsoft 365, Google Workspace, LMS	Data theft, service disruption	External attackers, insiders	Credential theft, API abuse, misconfigured cloud services

5. PREVENTION & PRECAUTIONARY MEASURES

The Cyber Crisis Management Plan (CCMP) of the Central University of Jammu is designed to strengthen the University's cyber resilience by enabling it to effectively anticipate, withstand, contain, recover from, and adapt to cyber security incidents. The framework focuses on the following key capabilities:

- **Anticipate:** Maintain a proactive state of cyber preparedness through continuous risk assessment, threat intelligence, vulnerability management, and security monitoring to prevent or minimize the impact of cyber threats.
- **Withstand:** Ensure the continuity of critical academic, administrative, and research services even when cyber attacks successfully compromise parts of the University's information systems.
- **Contain:** Rapidly detect, isolate, and contain affected systems to prevent the spread of cyber incidents while safeguarding trusted networks and maintaining essential University operations.
- **Recover:** Restore affected systems, services, and data in a timely manner to resume normal operations with minimal disruption following a cyber incident.
- **Evolve:** Continuously improve cyber security capabilities, policies, technologies, and response procedures by incorporating lessons learned from incidents, emerging threats, and evolving regulatory requirements.

Following measures are imperative to effectively manage cyber crises:

- Adoption of recognized cybersecurity standards, guidelines, and industry best practices.
- Regular security audits and vulnerability assessments of the University's IT infrastructure and network.
- Continuous monitoring and analysis of network traffic to identify malicious activities.
- Segmentation and isolation of critical systems and networks to limit the impact of cyber incidents.

- Compliance with cybersecurity advisories, standards, and guidelines issued by relevant government and regulatory authorities.
- Background verification of personnel with privileged access to critical information assets.
- Periodic audit, assurance, and compliance assessments to evaluate the effectiveness of security controls.
- Timely reporting and sharing of cyber threat intelligence and incident information with relevant authorities and internal stakeholders to facilitate coordinated response and mitigation.

6. MITIGATION STEPS

6.1. Web Application Attacks

Web application attacks target vulnerabilities in internet-facing applications such as university admission portals, Learning Management Systems (LMS), ERP systems, digital libraries, and payment gateways. Common attacks include SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE), and File Inclusion attacks. Successful exploitation can lead to unauthorized access, data theft, website defacement, or complete system compromise.

Mitigation Measures:

- Adopt Secure Software Development Lifecycle (SSDLC) practices.
- Conduct regular Vulnerability Assessment and Penetration Testing (VAPT).
- Validate and sanitize all user inputs.
- Implement parameterized queries to prevent SQL Injection.
- Apply security patches and updates promptly.
- Enable Multi-Factor Authentication (MFA) for administrative access.
- Maintain application logs and continuous security monitoring.

6.2. Distributed Denial of Service (DDoS) Attacks

A Distributed Denial of Service (DDoS) attack overwhelms a university's servers, applications, or network infrastructure by generating massive volumes of malicious traffic from multiple compromised devices (botnets). This exhausts system resources, making services such as admission portals, websites, LMS, or email systems unavailable to legitimate users.

Mitigation Measures:

- Deploy DDoS protection services and cloud-based scrubbing solutions.
- Configure firewalls and Intrusion Prevention Systems (IPS).
- Implement rate limiting and traffic filtering.
- Use Content Delivery Networks (CDNs) to distribute traffic.
- Maintain redundant internet connectivity.
- Monitor network traffic continuously using SIEM and IDS/IPS.
- Coordinate with Internet Service Providers (ISPs) during attacks.
- Develop and regularly test a DDoS response plan.

6.3. DNS Attacks

DNS attacks target the Domain Name System, disrupting the translation of domain names into IP addresses. Common DNS attacks include DNS Spoofing (Cache Poisoning), DNS Amplification, DNS Tunneling, and DNS Hijacking. These attacks can redirect users to malicious websites, disrupt university services, or facilitate data exfiltration.

Mitigation Measures:

- Deploy DNS Security Extensions (DNSSEC).
- Restrict recursive DNS queries.
- Use secure and trusted DNS service providers.
- Monitor DNS traffic for anomalies.
- Implement DNS filtering and reputation services.
- Configure Response Rate Limiting (RRL).
- Keep DNS servers patched and hardened.

6.4. Spam Attacks

Spam attacks involve sending large volumes of unsolicited emails containing advertisements, phishing links, malicious attachments, or malware. Spam can overload email systems, reduce productivity, and serve as a delivery mechanism for ransomware and credential theft.

Mitigation Measures:

- Deploy secure email gateways with anti-spam capabilities.
- Implement SPF, DKIM, and DMARC email authentication.
- Enable attachment and URL scanning.
- Block known malicious domains and IP addresses.
- Conduct regular phishing awareness training.
- Disable automatic execution of email attachments.
- Maintain updated anti-malware solutions.
- Report suspicious emails through an established incident reporting mechanism.

6.5. Social Engineering Attacks

Social engineering attacks manipulate individuals into revealing confidential information, transferring funds, or granting unauthorized system access. Attackers exploit human psychology rather than technical vulnerabilities. Common techniques include phishing, spear phishing, vishing (voice phishing), smishing (SMS phishing), impersonation, baiting, and pretexting.

Mitigation Measures:

- Conduct periodic cybersecurity awareness and training programs.
- Implement Multi-Factor Authentication (MFA).

- Verify requests involving sensitive information through secondary communication channels.
- Establish identity verification procedures.
- Promote a "Think Before You Click" culture.
- Restrict user privileges using the Principle of Least Privilege.
- Conduct simulated phishing exercises.
- Develop clear reporting procedures for suspicious communications.

6.6. Application Attacks

Application attacks exploit vulnerabilities in desktop, mobile, cloud-based, or enterprise applications used within the university. These attacks may target authentication mechanisms, insecure APIs, session management, software vulnerabilities, or misconfigurations to gain unauthorized access, execute malicious code, or steal sensitive information.

Mitigation Measures:

- Follow secure coding standards (e.g., OWASP Secure Coding Practices).
- Perform regular vulnerability assessments and penetration testing.
- Apply timely software patches and updates.
- Implement strong authentication and role-based access control (RBAC).
- Encrypt sensitive data both in transit and at rest.
- Conduct application security testing before deployment.
- Monitor application logs for suspicious activities.
- Deploy Endpoint Detection and Response (EDR) solutions.
- Regularly review third-party libraries and dependencies for vulnerabilities.

7. INCIDENT REPORTING PROCEDURES

Reporting of an Incident

Employees can report an adverse activity or unwanted behavior which they may feel as an incident to CSO.

Contents of Incident Report

The following information (as much as possible) may be given while reporting the incident:

- Time of occurrence of the incident
- Information regarding affected system / network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage.

Verification

Emergency Response Team (ERT) will verify the authenticity of the report.

Incident Response

The CSO and his team will assist in the incident handling:

Identification: To determine whether an incident has occurred, if so analyzing the nature of such incident, protection of evidence and reporting of the same.

Containment: To limit the scope of the incident quickly and minimize the damage.

Eradication: To remove the cause of the incident.

Recovery: Taking steps to restore normal operation.

Incident Reporting Form

Cyber Event / Incident should be reported in the defined format to the CSO.

Contact Information				
Name				
Place of Incident				
Email				
Mobile Number				
Event Occurance Details				
Date		Time		
Comments				
Physical Location of Affected System				
Type of Device	MAC Address	Serial Number	IP Address	Impact details
Incident Description				
Date of Last device update				
Is the device standalone or conencted to network				
System isolated from network after incident				
Has any similar problem occurred earlier				
Self-Control measures if any				