



JSS ACADEMY OF HIGHER EDUCATION & RESEARCH

RISK MANAGEMENT PLAN

Risk Management Policy and Enterprise Risk Management (ERM) Framework

EXECUTIVE SUMMARY

What is this policy about?

JSS Academy of Higher Education & Research (JSS AHER) is committed to a structured, integrated and proactive approach to identifying, assessing, mitigating and monitoring institutional risks. This Risk Management Policy and Enterprise Risk Management (ERM) Framework provides a common approach for strategic, academic, regulatory, clinical, research, operational, financial, technological, cybersecurity, campus safety, reputational and other institutional risks.

Who should follow this policy?

This framework applies across JSS AHER, including constituent colleges, academic departments, research centres, clinical facilities, administrative units, students, faculty, staff, researchers, contractors and other stakeholders whose activities may create or be affected by institutional risk.

How does the University oversee risk?

The Risk Management Committee (RMC), chaired by the Vice-Chancellor, provides university-wide oversight and undertakes quarterly reviews. The Institutional Risk Officer (IRO) coordinates risk-register updates across constituent units, while Deans, Principals and Medical Superintendents act as operational risk owners within their respective areas.

Purpose

The purpose of this policy is to embed risk management into institutional planning, governance and decision-making, strengthen resilience, protect students, patients, staff, research and institutional assets, and support the achievement of JSS AHER's strategic objectives.

1. RISK MANAGEMENT PRINCIPLES

- Risk management shall be integrated with strategic planning, quality assurance, operational planning and institutional decision-making.
- Risks shall be identified proactively through risk registers, cross-functional reviews, incident reporting, audits and horizon scanning.
- Each material risk shall have a clearly identified owner, mitigation actions and review arrangements.
- Risk responses may include resolving, reducing, transferring or accepting a risk, based on institutional risk appetite.
- High-severity risks shall be escalated promptly and shall not wait for the next scheduled committee meeting.
- Risk management shall support opportunities and innovation while protecting statutory, ethical, academic, clinical, financial and safety obligations.
- Risk registers and mitigation actions shall be reviewed periodically and updated when the risk profile changes.

2. CORE INSTITUTIONAL RISK CATEGORIES

3. RISK GOVERNANCE STRUCTURE

4. STRATEGIC, OPERATIONAL AND PROJECT RISK

Risk management shall operate at institutional, college/constituent-unit, department/service and project levels. Major projects and strategic initiatives shall maintain separate risk registers where appropriate. Risk information shall be consolidated for institutional review, with material risks escalated to the RMC.

Suggested review cycle:

- RMC – quarterly institutional risk review.
- Constituent colleges / major units – periodic review, with a full annual review.
- Departments and operational units – review at least quarterly or more frequently where risk exposure is high.
- Major projects – review at every project governance meeting.
- Critical incidents – immediate escalation without waiting for the scheduled review.

5. RISK IDENTIFICATION AND REGISTER

Each material risk should be documented using a consistent risk-register structure containing, at minimum:

- Risk ID and risk title
- Risk owner
- Root cause
- Risk description
- Potential impact / consequence
- Risk category and strategic alignment
- Initial likelihood and impact
- Current likelihood and impact
- Overall current risk rating
- Mitigation controls and actions
- Action owner and target date
- Residual likelihood and impact
- Risk movement: worsening, stable or improving
- Review date, status and supporting evidence
- Escalation level and committee responsible

6. RISK ASSESSMENT AND SCORING

For institutional consistency, JSS AHER may use a 5 × 5 likelihood-impact methodology. The numerical scoring approach below is an adaptation of the risk-register methodology reflected in the reference University of Glasgow framework; the institutional thresholds should be approved by the competent authority before formal implementation.

Risk score = Likelihood × Impact. Both current and residual risk should be recorded.

7. RISK RESPONSE AND MITIGATION

- RESOLVE – remove the source of risk where practicable.
- REDUCE – implement controls to reduce likelihood or impact.
- TRANSFER – transfer an appropriate element of the risk through insurance, contractual arrangements or specialist providers.
- ACCEPT – consciously accept the residual risk where it is within approved risk appetite and further treatment is disproportionate.
- EXPLOIT / ENABLE – where a risk represents an opportunity, consider controlled action that supports institutional improvement or innovation.

8. RISK APPETITE

JSS AHER shall maintain a differentiated risk appetite. The University should demonstrate minimal tolerance for risks that could compromise patient safety, student and staff safety, legal or regulatory compliance, research integrity, data protection, cybersecurity and institutional trust. A greater degree of managed risk may be considered for academic innovation, research, technology adoption, internationalisation and strategic development where there is a clear institutional benefit and appropriate controls.

9. ENTERPRISE RISK MANAGEMENT POLICY: INFORMATION TECHNOLOGY & CYBERSECURITY

Purpose

This policy establishes the framework for identifying, assessing and mitigating IT and cybersecurity risks at JSS AHER. It protects digital infrastructure, sensitive research data, student records, clinical information, intellectual property and operational continuity.

Scope

It applies to administrators, faculty, staff, researchers, students, contractors and external vendors accessing university IT resources, networks, hardware or data.

Access Control and Identity Management

Strict identity and access management shall be enforced. Multi-factor authentication shall be mandatory for institutional accounts accessing core administrative, financial and student systems. Access shall follow least-privilege principles.

Data Classification and Protection

Institutional data shall be classified as Public, Internal or Restricted/Confidential. Restricted data, including student financial records, medical histories and proprietary research, shall be encrypted at rest and in transit.

Monitoring and Vulnerability Assessment

Bi-annual vulnerability scans and annual external penetration testing should cover relevant network, server and application environments. Real-time monitoring should be used to detect anomalous activity.

Patch and Lifecycle Management

Security updates shall be deployed systematically. Critical security patches should be applied within 72 hours of release where technically feasible; unsupported systems should be isolated or decommissioned.

User Awareness and Training

Annual cybersecurity and data-protection training shall be completed by employees, supported by periodic phishing simulations and awareness campaigns.

Incident Response and Business Continuity

- An IT Security Incident Response Team (ISRT) shall maintain a documented incident response plan.
- Critical institutional data shall be backed up automatically, encrypted and stored in secure off-site or cloud-based environments.
- Backup restoration shall be tested at least quarterly for critical systems.
- Major cybersecurity incidents shall be escalated immediately through the institutional risk governance structure.

10. ENTERPRISE RISK MANAGEMENT POLICY: FINANCIAL PLANNING & BUDGETARY CONTROL

Purpose

To safeguard financial health, liquidity and long-term sustainability through structured budgeting, cost control and financial risk mitigation.

Scope

Covers financial operations, revenue streams, capital expenditure, research grants, endowment funds and departmental budgets across JSS AHER.

Conservative Revenue Forecasting

Annual budgets should use realistic, data-driven revenue projections and appropriately conservative enrolment assumptions.

Decentralized Budget Accountability

Deans and Heads shall prepare and defend annual budgets. Variances beyond approved thresholds shall require formal justification and appropriate prior approval.

Liquidity and Contingency Reserves

The University should maintain an appropriate operating contingency reserve, with access governed by approved institutional controls.

Capital Expenditure Evaluation

Major capital projects should undergo risk-adjusted ROI and cost-benefit assessment, with funding sources identified before major commitments.

Internal Controls and Separation of Duties

No single individual should initiate, approve and execute a financial transaction. Internal audits should cover procurement, payroll and asset management.

Compliance and Reporting

Periodic financial variance reports shall be submitted to leadership, and annual financial statements shall undergo independent external audit as required.

11. ENTERPRISE RISK MANAGEMENT POLICY: CAMPUS SAFETY & PHYSICAL SECURITY

Purpose

To maintain a safe, secure and resilient physical environment for students, faculty, staff, patients, visitors and other stakeholders.

Scope

Applies to campuses, residential facilities, laboratories, recreational areas, university transportation and off-campus institutional events.

Physical Access Control and Surveillance

Campus entry points shall be monitored by trained security personnel. Appropriate identification and CCTV systems shall be maintained for public perimeters and high-risk areas.

Laboratory and Hazardous Material Safety

Facilities using chemical, biological or radiological materials shall implement appropriate access controls, inventory records, safety protocols and periodic independent safety audits.

Emergency Communications

An integrated mass-notification mechanism should support rapid emergency alerts through appropriate channels including SMS, email, public-address systems and mobile platforms.

Infrastructure and Fire Safety

Buildings shall comply with applicable building, electrical and fire-safety requirements. Fire detection, alarms and suppression systems shall be inspected periodically by competent personnel.

Crisis Management and Emergency Drills

A campus crisis management plan shall be maintained in coordination with local emergency services. Emergency evacuation and lockdown drills should be conducted periodically.

Reporting and Review

An accessible mechanism shall be provided for reporting safety hazards and security concerns. The Campus Safety Committee shall review incident trends and corrective actions.

12. INSTITUTIONAL RISK MATRIX

13. MONITORING, REPORTING AND ESCALATION

- Quarterly Risk Registers: Department and unit heads shall update local risk registers and re-evaluate risk scores based on operational changes.

- Consolidated Institutional Risk Register: The IRO shall consolidate material risks for review by the RMC.
- Incident Escalation: Any high-severity event, including a major patient-safety incident or significant IT outage, shall be escalated to the RMC within 4 hours, or immediately where circumstances require.
- Risk Movement: Each review shall identify whether the risk is worsening, stable or improving.
- Mitigation Tracking: Every mitigation action shall have an accountable owner and target date; controls shall have defined review dates.
- Annual Independent Review: An independent review/audit should assess the maturity and effectiveness of the risk framework and inform strategic planning and budget allocation.
- Continuous Horizon Scanning: Emerging risks from regulatory, technological, clinical, academic, financial and geopolitical developments shall be monitored.

14. RISK REPORTING FORMAT

15. BUSINESS CONTINUITY AND RESILIENCE

JSS AHER shall maintain appropriate business continuity arrangements for critical academic, clinical, research, administrative and digital services. Continuity planning should identify critical functions, dependencies, recovery priorities, alternative arrangements, communication protocols and recovery testing requirements.

16. TRAINING AND RISK CULTURE

Risk management shall be embedded as an institutional culture rather than treated solely as a compliance exercise. Relevant personnel shall receive periodic training on risk identification, assessment, mitigation, incident reporting, cybersecurity, safety and business continuity. Leadership shall encourage timely reporting of emerging risks without discouraging responsible innovation.

17. POLICY REVIEW

This Risk Management Policy and ERM Framework should be reviewed at least annually, or earlier where significant changes occur in the regulatory, clinical, technological, financial or strategic environment. The review should consider lessons from incidents, audits, risk-register trends, emerging risks and changes in institutional strategy.

18. APPROVAL AND ACCOUNTABILITY

Prepared for institutional consideration and approval by the competent authority of JSS Academy of Higher Education & Research.

Registrar
JSS Academy of Higher Education & Research
Mysuru

ANNEXURE I – RISK MANAGEMENT PROCESS

ANNEXURE II – INSTITUTIONAL RISK GOVERNANCE FLOW

Department / Unit Risk Identification → Risk Owner Assessment → Constituent College / Unit Review → Institutional Risk Officer Consolidation → Risk Management Committee Review → Escalation to University Leadership / Competent Authority where required → Monitoring of Mitigation → Periodic Review and Assurance.

CONSOLIDATED INSTITUTIONAL RISK MATRIX

Risk Area	Principal Risk	Inherent	Residual	Key Controls / Mitigation
Academic & Regulatory	Non-compliance with UGC, NMC, PCI requirements or deterioration in accreditation/ranking standing	High	Low	IQAC audits, compliance monitoring and institutional dashboards
Clinical Operations	Medical errors, cross-contamination and patient-safety incidents	High	Medium	NABH-aligned protocols, clinical audits and morbidity/mortality reviews
Research Integrity	Biosafety breaches, ethics non-compliance, clinical-trial or IP leakage	High	Low	IBSC/IEC oversight, research governance and controlled access
Cybersecurity & Data	Ransomware, EHR/student data breach or major IT outage	High	Medium	RBAC, MFA, encryption, backups, vulnerability testing and incident response
Financial & Facilities	Funding interruption, infrastructure downtime or utility failure	Medium	Medium	Revenue diversification, contingency planning, backup systems and preventive maintenance
Strategic / Reputation	Failure to deliver strategic priorities or material reputational damage	High	Medium	Strategic monitoring, stakeholder engagement, escalation and corrective action
Campus Safety	Fire, security, laboratory or emergency-management failure	High	Low/Medium	Access control, CCTV, safety audits, drills and emergency communication

KEY RISK MANAGEMENT POLICIES

Information Technology & Cybersecurity

- Mandatory MFA for core institutional accounts and least-privilege access.
- Data classification as Public, Internal and Restricted/Confidential.
- Encryption of restricted data at rest and in transit.
- Biannual vulnerability scans, annual external penetration testing and real-time monitoring.
- Critical patches targeted within 72 hours where technically feasible.
- Annual cyber hygiene/data protection training and phishing simulations.
- IT Security Incident Response Team (ISRT), documented incident response plan and encrypted off-site/cloud backups.
- Quarterly restoration tests for critical systems.

Financial Planning & Budgetary Control

- Conservative, data-driven revenue forecasting.
- Decentralised budget accountability with formal variance justification.
- Appropriate liquidity and contingency reserves.
- Risk-adjusted ROI/cost-benefit assessment for major capital expenditure.

- Separation of duties and periodic internal audits.
- Periodic financial variance reporting and independent external audit.

Campus Safety & Physical Security

- Monitored campus access and identification controls.
- CCTV and appropriate retention for security monitoring.
- Laboratory hazardous-material controls and safety audits.
- Rapid emergency notification through appropriate channels.
- Building, electrical and fire-safety compliance and periodic inspections.
- Crisis management arrangements and evacuation/lockdown drills.
- Accessible incident reporting and periodic Campus Safety Committee review.

RISK REVIEW CYCLE

- Department and unit risk registers – at least quarterly and more frequently where exposure is high.
- Constituent colleges / major units – periodic review with a full annual review.
- Risk Management Committee – quarterly institutional review.
- Major projects – review at each project governance meeting.
- Critical incidents – immediate escalation without waiting for scheduled review.
- Annual independent review of risk framework maturity and effectiveness.

APPROVAL AND ACCOUNTABILITY

This Risk Management Plan and ERM Framework is prepared for institutional consideration and approval by the competent authority of JSS Academy of Higher Education & Research, Mysuru.




 Registrar
REGISTRAR
 JSS Academy of Higher Education & Research
 Sri Shivarathreeshwara Nagara
 Mysuru-570015, Karnataka, India