Action Plan 7 for Incident Response and Recovery

By following this action plan and checklist, higher education institutions can develop a robust incident response and recovery framework that enables prompt and effective handling of cybersecurity incidents, ensures minimal downtime and data loss, and enhances the institution's overall cybersecurity resilience.

1. Incident Response Team: Form a dedicated incident response team comprising cybersecurity experts, IT personnel, legal representatives, communication specialists, and relevant stakeholders from different departments.
2. Incident Response Plan (IRP): Develop a well-defined incident response plan that outlines the step-by-step procedures to be followed in the event of a cybersecurity incident. The plan should cover various types of incidents, such as data breaches, malware infections, denial-of-service attacks, and insider threats.
3. Roles and Responsibilities: Define clear roles and responsibilities for each member of the incident response team. Assign specific tasks to ensure a coordinated and efficient response during an incident.
4. Communication Protocols: Establish communication protocols to ensure that all stakeholders, including senior leadership, faculty, staff, students, and external partners, are informed promptly during an incident. Determine the appropriate channels for communication and escalation.
5. Incident Categorisation and Severity: Establish a system for categorising incidents based on their severity and impact. This categorisation will help prioritise responses and allocate resources effectively.
6. Training and Drills: Provide regular training and conduct simulated incident response drills to familiarise the incident response team with the plan and ensure they are prepared to respond effectively in real-world scenarios.
7. Data Backup and Recovery: Implement robust data backup and recovery strategies to minimise downtime and data loss during and after an incident. Regularly test data restoration processes to ensure their effectiveness.
8. Forensic Readiness: Prepare the infrastructure for forensic investigation by enabling logging, monitoring, and data capture capabilities to gather evidence in case of a security incident.
9. Containment and Mitigation: Establish procedures for containing and mitigating the impact of incidents promptly. Determine when to isolate affected systems, shut down services, or apply emergency patches.
10. Forensic Investigation: Develop procedures for conducting a thorough forensic investigation to identify the root cause of the incident, assess the extent of the breach, and collect evidence for legal or regulatory purposes.
11. Coordination with Law Enforcement: Establish protocols for collaborating with law enforcement agencies, if necessary, during an incident, especially for major cybersecurity breaches.
12. Post-Incident Review: Conduct post-incident reviews after each cybersecurity incident to evaluate the effectiveness of the response, identify areas for improvement, and update the incident response plan accordingly.
13. Continuous Improvement: Continuously update the incident response plan based on lessons learned from incidents, changes in the threat landscape, and industry best practices.
14. Incident Reporting and Documentation: Maintain detailed records of all incidents, including incident reports, logs, evidence, and actions taken during the response and recovery process.

Action Plan 7 Checklist

✅ Formed a dedicated incident response team.

✅ Developed a well-defined incident response plan (IRP).

✅ Defined clear roles and responsibilities for the team members.

✅ Established communication protocols for all stakeholders.

✅ Categorised incidents based on severity and impact.

✅ Provided training and conducted incident response drills.

✅ Implemented robust data backup and recovery strategies.

✅ Prepared the infrastructure for forensic investigation.

✅ Established procedures for containment and mitigation.

✅ Developed protocols for forensic investigation.

✅ Established coordination with law enforcement, if necessary.

✅ Conducted post-incident reviews and updates to the IRP.

✅ Ensured continuous improvement of incident response capabilities.

✅ Maintained detailed incident reporting and documentation.