Action Plan 6 for Secure Infrastructure

By following this action plan and checklist, higher education institutions can create a secure infrastructure that protects against cyber threats, ensures data confidentiality and integrity, and maintains the institution's ability to deliver its services effectively and securely.

1. Infrastructure Assessment: Conduct a comprehensive assessment of the institution's IT infrastructure, including networks, systems, servers, endpoints, and devices, to identify existing security measures and potential vulnerabilities.
2. Network Security: Implement robust network security measures, such as firewalls, intrusion prevention systems (IPS), and virtual private networks (VPNs), to protect against unauthorised access and network-based attacks.
3. Endpoint Protection: Deploy endpoint security solutions, including antivirus/anti-malware software, host intrusion prevention, and endpoint detection and response (EDR) tools, to safeguard individual devices from malware and other threats.
4. Data Encryption: Implement data encryption for sensitive data both in transit and at rest to protect against data interception and unauthorised access.
5. Patch Management: Establish a proactive patch management process to ensure that operating systems, applications, and firmware are regularly updated with the latest security patches and updates.
6. Multi-Factor Authentication (MFA): Enforce the use of multi-factor authentication for accessing critical systems and resources to add an extra layer of security against unauthorised access.
7. Security Monitoring and Logging: Set up robust security monitoring and logging mechanisms to detect and respond to security incidents promptly. Monitor network traffic, user activities, and system logs for signs of suspicious behaviour.
8. Security Incident and Event Management (SIEM): Implement a SIEM system to aggregate, correlate, and analyse security events across the infrastructure to identify potential threats and security incidents.
9. Regular Vulnerability Assessments: Conduct regular vulnerability assessments to identify weaknesses and potential entry points in the IT infrastructure. Use reputable scanning tools and techniques to identify vulnerabilities.
10. Penetration Testing: Perform periodic penetration testing to simulate real-world attacks and test the effectiveness of security controls and incident response capabilities.
11. Security Awareness Training: Provide regular security awareness training for IT staff and end-users to educate them about cybersecurity best practices and the role they play in maintaining a secure infrastructure.
12. Incident Response Plan: Develop a comprehensive incident response plan to define the steps to be taken in the event of a security breach or incident. Establish roles, responsibilities, and communication protocols for incident handling.
13. Backup and Disaster Recovery: Implement regular data backups and a robust disaster recovery plan to ensure the availability and integrity of critical data in case of data loss or system failure.
14. Continuous Improvement: Continuously review and update security measures based on emerging threats, industry best practices, and lessons learned from security incidents.

Action Plan 6 Checklist

✅ Conducted a comprehensive infrastructure assessment.

✅ Implemented robust network security measures.

✅ Deployed endpoint protection solutions.

✅ Implemented data encryption for sensitive data.

✅ Established a proactive patch management process.

✅ Enforced multi-factor authentication (MFA).

✅ Set up security monitoring and logging mechanisms.

✅ Implemented a Security Incident and Event Management (SIEM) system.

✅ Conducted regular vulnerability assessments.

✅ Performed periodic penetration testing.

✅ Provided security awareness training for IT staff and end-users.

✅ Developed a comprehensive incident response plan.

✅ Implemented regular data backups and a disaster recovery plan.

✅ Ensured continuous improvement of security measures.