




Security Management Policy

Version 1.0

October 2023

Ver No.	Policy	Prepared By	Reviewed By	Signature Approval	Date Signed
1	Security Management Policy	Omar	Mehad Ul Haque & Ivdad Ahmed Khan Mojlish		Oct 30, 2023

1. Purpose and Scope:

The purpose of this Security Management Policy is to establish guidelines and procedures to ensure the confidentiality, integrity, and availability of information assets at LightCastle Partners Limited. This policy applies to all employees, contractors, and third-party entities with access to LightCastle's information systems.

2. Information Security Objectives:

Protect the confidentiality of sensitive information.

Ensure the integrity of data and information.

Guarantee the availability of information systems.

Comply with legal and regulatory requirements.

Safeguard the reputation and trust of LightCastle Partners Limited.

Minimize the risk of security breaches and incidents.

3. Information Classification:

All information assets shall be classified based on their sensitivity and criticality. Classification levels include Public, Internal Use Only, Confidential, and Restricted. Access controls and protective measures will be applied according to the classification.

4. Access Control:

User access rights will be granted based on the principle of least privilege.

Access to sensitive information will be restricted and monitored.

User account management will follow strict procedures, including timely deactivation of accounts for terminated employees.

5. Data Encryption:

Sensitive data in transit and at rest must be encrypted using industry-standard encryption algorithms and protocols to prevent unauthorized access.

6. Network Security:

Firewalls and intrusion detection/prevention systems will be implemented to protect the network infrastructure.

Wireless networks will be secured using strong encryption and access controls.

Regular vulnerability assessments and penetration testing will be conducted.

7. Physical Security:

Physical access to data centres, server rooms, and other critical infrastructure will be restricted and monitored.

Surveillance cameras and access control systems will be deployed in sensitive areas.

8. Incident Response:

An incident response plan will be established to detect, respond to, and recover from security incidents. This includes reporting procedures, incident analysis, and communication protocols.

9. Security Awareness Training:

All employees will receive regular training on security best practices, policies, and procedures to ensure a high level of security awareness.

10. Compliance:

LightCastle Partners Limited will comply with relevant legal and regulatory requirements related to information security. Regular audits and assessments will be conducted to ensure compliance.

11. Security Monitoring:

Continuous monitoring of information systems and network activities will be performed to detect and respond to security threats and vulnerabilities promptly.

12. Security Policy Review:

This Security Management Policy will be reviewed annually or as needed to ensure its relevance and effectiveness.

13. Responsibilities:

The Chief Information Security Officer (CISO) is responsible for the overall implementation and enforcement of this Security Management Policy. All employees are responsible for adhering to the policies and reporting any security concerns promptly.

14. Enforcement:

Violations of this Security Management Policy may result in disciplinary action, including but not limited to reprimands, suspension, termination, and legal action, as deemed appropriate.

15. Policy Distribution:

This policy will be distributed to all employees and contractors and will be made available on the company's intranet.

16. Security Controls for Mobile Devices:

Mobile devices used for business purposes will be configured with appropriate security settings, including encryption and password protection.

Mobile device management (MDM) solutions will be implemented to enforce security policies on mobile devices.

17. Remote Access Security:

Secure remote access methods, such as virtual private networks (VPNs), will be utilized for accessing company systems remotely.

Multi-factor authentication (MFA) will be enforced for remote access to enhance authentication security.

18. Third-Party Security:

Third-party vendors and partners with access to LightCastle's systems will be required to adhere to security standards and undergo periodic security assessments.

Contracts with third parties will include security clauses and requirements.

19. Security Incident Reporting:

All employees are required to report any suspected or confirmed security incidents promptly to the IT or Security team.

An incident response team will be designated and trained to handle security incidents effectively.

20. Data Backup and Recovery:

Regular backups of critical data will be performed, and the integrity and effectiveness of backups will be tested periodically.

A documented data recovery plan will be in place to minimize downtime in the event of data loss or system failures.

21. Change Management:

Changes to information systems, applications, or network configurations will follow a formal change management process.

The impact of changes on security will be assessed, and necessary security measures will be implemented.

22. Business Continuity and Disaster Recovery:

Business continuity and disaster recovery plans will be established to ensure the continued operation of critical business processes in the event of a disruptive incident.

Regular testing and updating of these plans will be conducted to ensure their effectiveness.

23. Social Engineering Awareness:

Employees will receive training on recognizing and preventing social engineering attacks, such as phishing and pretexting.

Simulated phishing exercises may be conducted periodically to assess and improve employee awareness.

24. Emerging Threats and Technology Monitoring:

The IT and Security team will stay informed about emerging threats and technological advancements to proactively address new security challenges.

Security controls will be updated to mitigate risks associated with evolving threats.

25. Security Metrics and Reporting:

Key security metrics will be monitored and reported regularly to executive management to demonstrate the effectiveness of the security program.

Continuous improvement initiatives will be driven by analyzing security metrics and identifying areas for enhancement.

26. Privacy Protection:

LightCastle Partners Limited is committed to protecting the privacy of individuals and will comply with applicable data protection laws and regulations.

Privacy impact assessments will be conducted for new projects involving personal information.

27. Training and Awareness Program Evaluation:

The effectiveness of the security training and awareness program will be periodically evaluated through assessments and feedback from employees.

28. Collaboration with Law Enforcement:

In the event of a security incident, LightCastle Partners Limited will collaborate with law enforcement agencies as necessary to investigate and resolve the incident.

29. International Security Compliance:

For operations conducted in multiple jurisdictions, the security program will comply with the relevant international security standards and regulations.

30. Document Retention and Destruction:

Document retention policies will be established to define the storage and disposal of sensitive information in compliance with legal and regulatory requirements.

31. Cloud Security:

Security measures will be implemented to protect data stored in cloud environments, including the use of encryption, access controls, and regular security assessments.

32. Security Training for Development Teams:

Development teams will receive security training to ensure that secure coding practices are followed, and potential vulnerabilities are minimized.

33. Environmental Controls:

Measures will be implemented to safeguard information systems and data against environmental threats such as fire, flood, and other natural disasters.

34. Employee Exit Procedures:

When an employee leaves the company, a comprehensive exit procedure will be followed to revoke access rights, collect company property, and ensure the return of any sensitive information.

35. Security Program Review and Improvement:

The security program will undergo regular reviews to identify areas for improvement, and the policy will be updated accordingly.

36. Legal Compliance:

LightCastle Partners Limited is committed to complying with all applicable laws and regulations of the People's Republic of Bangladesh related to information security and data protection.

The security program will be designed and implemented in accordance with the Bangladesh Cyber Security Act and any other relevant legislation.

37. Data Protection and Privacy:

LightCastle Partners Limited recognizes the importance of protecting personal information and will comply with the provisions of the Bangladesh Data Protection Act, if applicable.

Any processing of personal data will be conducted in accordance with the principles and requirements outlined in the applicable data protection laws of Bangladesh.

38. Reporting of Security Incidents to Authorities:

In the event of a security incident that involves a breach of personal information, LightCastle Partners Limited will adhere to reporting requirements stipulated by the Bangladesh Telecommunication Regulatory Commission (BTRC) and other relevant authorities.

39. Compliance with Telecommunication Regulations:

All information systems and communication networks operated by LightCastle Partners Limited will adhere to the regulations set forth by the Bangladesh Telecommunication Regulatory Commission (BTRC) to ensure lawful and secure communication.

40. Security Audits and Assessments:

Periodic security audits and assessments will be conducted to ensure compliance with local regulations and standards, including those prescribed by the Bangladesh Computer Council (BCC) or any other relevant regulatory body.

41. Employee Training on Bangladesh Cyber Laws:

Employees will receive training on the specific provisions of Bangladesh's cyber laws, including the Cyber Security Act, to enhance awareness and understanding of legal responsibilities in the digital environment.

42. Collaboration with Government Agencies:

LightCastle Partners Limited will collaborate with relevant government agencies, such as the Bangladesh Telecommunication Regulatory Commission (BTRC) and the Bangladesh Computer Incident Response Team (CIRT), in the event of a significant security incident.

43. Cross-Border Data Transfer Compliance:

Cross-border transfer of data will be conducted by the regulations set forth by the Bangladesh Data Protection Act, ensuring that data subjects' rights are protected during international data transfers.

44. Vendor and Third-Party Compliance:

Third-party vendors and partners will be vetted for compliance with Bangladesh's legal and regulatory requirements, and contracts will include clauses to ensure adherence to local laws.

45. Local Incident Response Protocols:

Incident response procedures will include specific steps to be taken in compliance with Bangladesh's legal requirements, including reporting procedures to law enforcement and regulatory authorities.

46. Consumer Rights Protection:

LightCastle Partners Limited will respect and protect the rights of consumers as outlined in the Consumer Rights Protection Act of Bangladesh, particularly concerning the security and privacy of consumer data.

47. Regulatory Changes Notification:

The security program will be adapted promptly to any changes in the legal and regulatory landscape of Bangladesh, and employees will be informed of such changes that impact their roles and responsibilities.