Application and Physical Security

Hex Secure Framework

VERSION: 1.2 REVISION DATE: Apr 18, 2025

Contents

Section 1 Purpose

The purpose of this document is to define Hexagon Group's Application and Physical Security policies. These policies are essential for safeguarding information systems, preventing unauthorized access, and ensuring operational continuity across physical and digital environments.

Section 2 Application Security

2.1 Third-Party Software Update

- All third-party software must be reviewed and updated regularly to patch vulnerabilities.
- Software updates must be approved and documented by the application security team.

2.2 Email Security

- Emails must pass through spam filters and advanced threat protection.
- All employees must undergo training on phishing detection and safe email handling.

2.3 New Application Risk Assessment

- All new applications must undergo a security risk assessment before deployment.
- The assessment includes threat modeling, code analysis, and compliance checks.

Section 3 Physical Security

3.1 Access Control

- Only authorized personnel are allowed into critical areas using keycards or biometric systems.

-Personnel for example can have access such as:security officers, high-level technicians, IT personnel, etc.

- Access logs must be maintained and reviewed weekly by the security officer.

3.2 Surveillance

- CCTV cameras must cover all entry points and server rooms.

- Also including 2-5 security guards by day, and 1-2 security guards on shift by night depending the size and scale of the physical infrastructure

- Footage is stored securely for a minimum of 30 days and reviewed in case of incidents.

3.3 Alarm and Alert System

- Intrusion detection alarms must be installed at strategic points.
- Alarms are integrated with the central monitoring system for real-time response.

Section 4 Implementation and Monitoring

4.1 Application Security Implementation

- Security baselines are applied through automation and configuration tools.
- Logs from apps and email filters are centralized and monitored.

4.2 Physical Security Monitoring

- Security guards patrol during off-hours and respond to alarms.
- Monitoring dashboards track surveillance system health and coverage.

4.3 Compliance and Audits

- Internal audits are conducted quarterly to ensure adherence.
- Any deviation from policy is escalated to IT security leadership.

Section 10 References

Document No.	Document Title	Date	Author