Kemicard Practical Information Security Policy and Client Assurance

1. Governance

1.1 Information Security Program

Kemicard maintains an internal Information Security Program designed to safeguard systems and client data. The program outlines security practices and team responsibilities across daily operations.

1.2 Policy Review

Information security policies are reviewed internally every two years or earlier if material changes occur in business operations, technology, or regulations. The Information Security Manager initiates this review and proposes updates.

1.3 Information Security Responsibility

Kemicard designates an Information Security Manager responsible for overseeing security practices, training, incident tracking, and continuous improvement. The role ensures that policies are known, practical, and followed.

1.4 IT Management Support

Security policies are drafted by the Information Security Manager and reviewed and approved by the leadership team. IT management ensures that security controls are practical and can be applied by operational teams.

1.5 Monitoring Regulatory Changes

Kemicard monitors significant regulatory trends through reputable online security resources. Any identified changes that may impact operations are evaluated and incorporated into practices during policy reviews.

2. Risk Management

2.1 Internal Security Reviews

Kemicard conducts internal security reviews of systems, applications, and access rights at least annually. Reviews are documented, and corrective actions are assigned and tracked to closure.

2.2 Change Management

All planned changes to production systems must be:

- Documented in a Change Request form.
- Reviewed for security, performance, and operational impacts.
- Approved by an IT Manager.
- Implemented during scheduled maintenance windows.

Emergency changes must be documented retroactively within 48 hours and reviewed post-implementation.

2.3 Risk Identification and Mitigation

Internal risk assessments are performed annually, identifying and rating risks based on impact and likelihood. Appropriate controls are implemented or updated based on assessment outcomes.

3. Security Awareness and Training

3.1 New Hire and Annual Security Training

All employees and contractors complete mandatory security training within 30 days of onboarding and annually thereafter.

Training includes:

- Password security
- Safe internet and email usage
- Recognizing and reporting phishing
- Physical security measures
- Incident reporting procedures

Training participation is recorded and monitored.

3.2 Confidentiality Agreements

All employees and contractors sign confidentiality agreements before being granted access to Kemicard’s systems and information.

3.3 Phishing Awareness

Kemicard conducts phishing awareness briefings during annual security refreshers. Spot-check simulations may be used to maintain vigilance.

4. Vulnerability Management and Patching Policy

4.1 Internal Vulnerability Management Process

Kemicard's internal IT team performs vulnerability scanning on all servers, workstations, and network devices at least quarterly. The vulnerability management process includes:

- **Identification**: Regular scans using approved tools.
- **Risk Assessment**: Vulnerabilities are categorized as Critical, High, Medium, or Low.
- **Remediation Plan**:
  - Critical vulnerabilities remediated within 15 business days.
  - High-risk vulnerabilities remediated within 30 business days.
  - Medium and low-risk vulnerabilities addressed during standard maintenance.
- **Verification**: Rescanning after remediation to confirm closure.

4.2 Patch Management Policy

Patches for operating systems, middleware, and key applications are reviewed monthly.

- **Patch Evaluation**:
  - Security patches are prioritized.
  - Business-critical systems are tested in a staging environment before live deployment when practical.
- **Deployment Schedule**:
  - Critical security patches deployed within 14 days of release.
  - Important security patches within 30 days.
  - Routine updates bundled into quarterly maintenance.

Emergency patching may occur outside scheduled windows based on threat intelligence.

Team members must document patch deployments and track pending updates until full completion.

5. Malware and Virus Protection

5.1 Endpoint Protection

All endpoints (workstations, laptops, servers) must have centrally managed antivirus and antimalware protection enabled with real-time scanning and automatic updates.

5.2 Email and Web Protection

Inbound and outbound emails are scanned for malicious content. Web browsing activity is filtered to block access to known malicious websites.

5.3 Mobile Device Security

All laptops must have disk encryption, active endpoint protection, and remote wipe capability. Lost or stolen devices must be reported within 24 hours.

6. Security Incident / Breach Response Plan

6.1 Incident Reporting Procedures

Any employee who identifies or suspects a security incident (e.g., unauthorized access, loss of equipment, suspicious emails) must immediately:

- Report the incident to the Information Security Manager by email and internal ticketing system.
- Preserve any evidence (e.g., do not shut down affected systems if possible).

Initial notification must include:

- Time and method of detection
- Description of suspected incident
- Systems and data involved

6.2 Incident Classification

Incidents are classified based on:

- **Minor**: No actual data compromise or system integrity issues.
- **Major**: Possible exposure or compromise of sensitive information or disruption of services.
- **Critical**: Confirmed data breach, system intrusion, or significant business disruption.

6.3 Incident Response Actions

Upon classification, the Information Security Manager coordinates the following:

- **Containment**: Isolate affected systems where applicable.
- **Eradication**: Remove malicious code, disable unauthorized accounts, repair vulnerabilities.
- **Recovery**: Restore systems and services after ensuring threats have been neutralized.
- **Communication**: Notify management and impacted parties based on the severity level.
- **Documentation**: Maintain a detailed incident report including timeline, actions taken, and lessons learned.

6.4 Forensics

If major or critical incidents occur, Kemicard conducts internal forensic investigations to:

- Identify the root cause
- Assess scope of impact
- Support corrective and preventive actions

External forensic services may be engaged if required for complex incidents.

6.5 Client Notification Policy

If an incident involves client data:

- Clients will be notified within 72 hours of incident confirmation.
- A preliminary report will be provided detailing known facts and interim mitigation steps.
- Ongoing updates will be provided as new information becomes available until incident closure.

6.6 Post-Incident Review

Following incident resolution, a post-incident review meeting is conducted to:

- Analyze root causes
- Identify gaps in policies or controls
- Implement enhancements to prevent recurrence

Findings from the review are documented and tracked until completed.

Document Owner: Information Security Manager
Last Reviewed: April 29, 2025
Next Review Date: May 1, 2027