

CLOUDGUARD TECHNOLOGIES INC.

Information Security & Data Privacy Policy

Vendor Security Documentation

Document Version:	2.4
Effective Date:	January 1, 2025
Last Updated:	December 15, 2024
Classification:	Confidential - For Client Review
Prepared For:	Third-Party Vendor Assessment

Table of Contents

1. Executive Summary
2. Company Overview
3. Data Protection & Encryption
4. Access Controls & Authentication
5. Business Continuity & Disaster Recovery
6. Compliance & Certifications
7. Incident Response & Security Operations
8. Vendor Management & Supply Chain Security
9. Physical & Environmental Security
10. Security Governance & Risk Management

1. Executive Summary

CloudGuard Technologies Inc. is a leading cloud infrastructure and managed services provider, serving enterprise clients across financial services, healthcare, and technology sectors. This security policy documentation outlines our comprehensive approach to information security, data protection, and regulatory compliance.

Our security program is built on industry best practices and frameworks including ISO 27001, NIST Cybersecurity Framework, and SOC 2 Type II requirements. We maintain a defense-in-depth approach with multiple layers of security controls protecting customer data and systems.

Security Measure	Implementation Status
ISO 27001 Certification	Current - Renewed Nov 2024
SOC 2 Type II Attestation	Current - Issued Oct 2024
GDPR Compliance	Full Compliance
HIPAA Compliance	Full Compliance (BAA Available)
PCI DSS Level 1	Certified Service Provider
Annual Penetration Testing	Completed Q4 2024
24/7 Security Operations Center	Active

2. Company Overview

2.1 Service Description

CloudGuard Technologies provides comprehensive cloud infrastructure, platform services, and managed security solutions. Our primary service offerings include:

- Cloud Infrastructure as a Service (IaaS) - Secure, scalable compute, storage, and networking resources
- Managed Security Services - 24/7 security monitoring, threat detection, and incident response
- Data Protection Services - Encryption, backup, disaster recovery, and data residency solutions
- Compliance Management - Audit support, policy development, and regulatory compliance tools

2.2 Data Center Locations

We operate Tier III and Tier IV certified data centers in the following regions:

Region	Location	Tier	Certifications
North America	Virginia, USA	Tier IV	ISO 27001, SOC 2, PCI DSS
North America	Oregon, USA	Tier III	ISO 27001, SOC 2
Europe	Frankfurt, Germany	Tier IV	ISO 27001, SOC 2, GDPR
Europe	Dublin, Ireland	Tier III	ISO 27001, SOC 2, GDPR
Asia Pacific	Singapore	Tier III	ISO 27001, SOC 2

3. Data Protection & Encryption

3.1 Encryption Standards

All customer data is protected using industry-leading encryption standards at multiple layers:

Data State	Encryption Method	Key Length	Algorithm
Data at Rest	AES Encryption	256-bit	AES-256-GCM
Data in Transit	TLS/SSL	2048-bit RSA	TLS 1.3
Database Encryption	Transparent Data Encryption	256-bit	AES-256
Backup Encryption	AES Encryption	256-bit	AES-256-CBC
Key Storage	Hardware Security Module	4096-bit	RSA-4096

3.2 Key Management

Our cryptographic key management follows NIST SP 800-57 guidelines. All encryption keys are stored in FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs). Key rotation occurs automatically every 90 days for data encryption keys and annually for key encryption keys. Customer-managed keys (CMK) are supported for organizations requiring additional control.

3.3 Data Residency and Sovereignty

Customers can select specific geographic regions for data storage and processing. Data residency commitments are contractually guaranteed and enforced through technical controls. Cross-border data transfers comply with applicable regulations including GDPR Standard Contractual Clauses and Privacy Shield frameworks where applicable.

3.4 Data Breach Notification

In the event of a confirmed security incident affecting customer data, CloudGuard commits to:

- Initial notification within 24 hours of incident confirmation
- Detailed incident report within 72 hours including scope, affected data, and remediation steps
- Regular updates throughout incident investigation and resolution
- Post-incident report within 30 days including root cause analysis and preventive measures
- Compliance with all applicable breach notification regulations (GDPR, HIPAA, state laws)

4. Access Controls & Authentication

4.1 Authentication Mechanisms

CloudGuard implements multi-layered authentication controls for all system access:

Access Type	Authentication Method	MFA Required	Session Timeout
Customer Portal	SSO/SAML 2.0	Yes	15 minutes idle
API Access	OAuth 2.0 + API Keys	Yes	60 minutes
Administrative Access	Certificate + Hardware Token	Yes	10 minutes idle
Support Access	SSO + Biometric	Yes	30 minutes idle
Emergency Access	Break-glass + MFA	Yes	5 minutes

4.2 Privilege Management

Access privileges are granted based on least privilege principles and role-based access control (RBAC). All privileged access requires additional approval and is subject to quarterly review. Segregation of duties is enforced for critical operations including production deployments, financial transactions, and security configuration changes.

4.3 Password Policy

- Minimum length: 14 characters
- Complexity: Must include uppercase, lowercase, numbers, and special characters
- Expiration: 90 days for standard users, 60 days for privileged users
- History: Cannot reuse last 12 passwords
- Lockout: Account locked after 5 failed attempts for 30 minutes
- Password managers: Approved and encouraged for all users

4.4 Audit Logging

Comprehensive audit logs are maintained for all system access and administrative activities. Logs include authentication attempts, privilege escalation, data access, configuration changes, and API calls. All logs are encrypted, tamper-proof, and retained for a minimum of 7 years. Real-time monitoring and alerting is implemented for suspicious activities.

Log data includes: timestamp, user identity, source IP address, action performed, affected resources, and success/failure status. Logs are reviewed daily by automated systems and weekly by security personnel.

5. Business Continuity & Disaster Recovery

5.1 Service Level Agreements

Service Tier	Uptime SLA	RTO	RPO	Support Response
Enterprise Premium	99.99%	1 hour	15 minutes	15 min (24/7)
Business	99.95%	4 hours	1 hour	1 hour (24/7)
Standard	99.9%	8 hours	4 hours	4 hours (business)

5.2 Backup Strategy

Automated backups are performed according to the following schedule:

- Full backups: Daily at 02:00 UTC
- Incremental backups: Every 6 hours
- Transaction log backups: Every 15 minutes
- Backup retention: 30 days online, 7 years archived
- Geographic redundancy: Backups replicated to minimum 3 separate regions
- Backup testing: Monthly automated restore testing, quarterly full DR drill

5.3 Disaster Recovery Capabilities

Our disaster recovery infrastructure provides automated failover capabilities with geographically distributed hot standby environments. All critical systems maintain active-active or active-passive redundancy across multiple availability zones and regions.

DR testing is conducted quarterly with full simulations including customer communication protocols. Annual third-party DR audit validates recovery procedures and documentation.

5.4 Business Continuity Planning

Comprehensive Business Continuity Plans (BCP) cover scenarios including natural disasters, cyber attacks, power outages, and pandemic events. Plans are reviewed and updated quarterly. Key personnel maintain emergency contact procedures and incident escalation protocols are documented and tested.

6. Compliance & Certifications

6.1 Current Certifications

Certification	Status	Scope	Last Audit	Next Audit
ISO 27001:2022	Active	All Services	Nov 2024	Nov 2025
SOC 2 Type II	Active	All Services	Oct 2024	Oct 2025
PCI DSS v4.0	Active	Payment Processing	Sep 2024	Mar 2025
HIPAA	Compliant	Healthcare Services	Aug 2024	Aug 2025
ISO 27017	Active	Cloud Security	Nov 2024	Nov 2025
ISO 27018	Active	Privacy Protection	Nov 2024	Nov 2025

6.2 Regulatory Compliance

CloudGuard maintains compliance with the following regulatory frameworks:

- GDPR (General Data Protection Regulation) - Full compliance including data subject rights, privacy by design, and DPO appointment
- CCPA/CPRA (California Consumer Privacy Act) - Consumer rights and data handling procedures
- HIPAA/HITECH - Business Associate Agreements available, comprehensive safeguards
- SOX (Sarbanes-Oxley) - Financial controls and audit trail requirements
- GLBA (Gramm-Leach-Bliley) - Financial data protection for banking clients
- FedRAMP (in progress) - Expected authorization Q2 2025

6.3 Third-Party Attestations

Independent security assessments are conducted annually by qualified third-party auditors. SOC 2 Type II reports are available under NDA to qualified customers. Penetration testing is performed quarterly by independent security firms with results remediated according to severity within defined SLAs (Critical: 48 hours, High: 7 days, Medium: 30 days).

7. Incident Response & Security Operations

7.1 Security Operations Center

CloudGuard operates a 24/7/365 Security Operations Center (SOC) staffed by certified security analysts. The SOC provides continuous monitoring, threat detection, and incident response capabilities using industry-leading SIEM, IDS/IPS, and threat intelligence platforms.

7.2 Incident Response Procedures

Our incident response program follows NIST SP 800-61 guidelines with defined procedures for detection, analysis, containment, eradication, and recovery. Incident severity levels determine response timeframes:

Severity	Definition	Response Time	Customer Notification
Critical	Data breach, ransomware, complete service outage	15 minutes	Immediate
High	Attempted breach, partial outage, data integrity issue	1 hour	Within 4 hours
Medium	Policy violation, malware detected, degraded performance	4 hours	Within 24 hours
Low	Minor security event, no customer impact	24 hours	Monthly summary

7.3 Threat Intelligence and Monitoring

We maintain subscriptions to multiple commercial and open-source threat intelligence feeds. Indicators of Compromise (IOCs) are automatically integrated into our security infrastructure. Real-time monitoring includes:

- Network traffic analysis and anomaly detection
- Endpoint detection and response (EDR) on all systems
- Cloud security posture management (CSPM)
- User and entity behavior analytics (UEBA)
- Automated vulnerability scanning and patch management

7.4 Communication Protocols

During security incidents, customers are notified through encrypted email to designated contacts and via the customer portal. A dedicated incident hotline provides 24/7 escalation capabilities. Post-incident reviews are conducted with affected customers and detailed reports provided including timeline, impact assessment, root cause, and preventive measures.

8. Vendor Management & Supply Chain Security

8.1 Third-Party Risk Management

All vendors and subcontractors undergo rigorous security assessments before engagement. Our vendor management program includes:

- Comprehensive security questionnaires and due diligence
- Review of vendor certifications and compliance status
- Contractual security requirements and right-to-audit clauses
- Annual security reassessments for critical vendors
- Supply chain risk analysis and dependency mapping
- Vendor performance monitoring and incident tracking

8.2 Critical Vendor Categories

Vendor Type	Security Requirements	Review Frequency
Cloud Infrastructure	SOC 2 Type II, ISO 27001	Quarterly
Software Components	SBOM, vulnerability disclosure, SDLC security	Quarterly
Security Tools	Independent validation, data handling agreements	Annually
Professional Services	Background checks, NDA, training certification	Annually

9. Physical & Environmental Security

9.1 Data Center Physical Controls

All CloudGuard data centers implement multiple layers of physical security:

- Perimeter security with 24/7 armed guards and vehicle barriers
- Biometric access control with mantrap portals
- Continuous video surveillance with 90-day retention
- Visitor escort requirements and comprehensive logging
- Motion sensors and intrusion detection systems
- Environmental monitoring for temperature, humidity, water detection

9.2 Environmental Controls

Critical infrastructure includes redundant power systems with N+1 UPS configuration, diesel generators with 72-hour fuel capacity, and automated transfer switches. Climate control maintains optimal temperature (68-72°F) and humidity (40-60%) with redundant HVAC systems. Fire suppression uses clean agent systems to protect equipment while ensuring personnel safety.

9.3 Asset Management

All hardware assets are tracked through lifecycle management system with unique identifiers. Secure decommissioning procedures include cryptographic erasure for storage media (NIST 800-88) and certificate of destruction. Failed drives are physically destroyed on-site under video surveillance.

10. Security Governance & Risk Management

10.1 Security Organization

CloudGuard's security program is led by the Chief Information Security Officer (CISO) who reports directly to the CEO. The security organization includes dedicated teams for security operations, risk management, compliance, and security engineering. A Security Steering Committee meets monthly to review risk posture and strategic initiatives.

10.2 Policy Framework

Comprehensive security policies cover all aspects of information security and are reviewed annually. Policies are approved by executive leadership and communicated to all personnel. Key policies include:

- Information Security Policy
- Acceptable Use Policy
- Data Classification and Handling Policy
- Incident Response Policy
- Business Continuity Policy
- Vendor Management Policy
- Change Management Policy
- Encryption and Key Management Policy

10.3 Security Awareness Training

All employees complete security awareness training during onboarding and annually thereafter. Specialized role-based training is provided for personnel with elevated access. Monthly security awareness campaigns address current threats. Simulated phishing exercises are conducted quarterly with results tracked and used for targeted training.

10.4 Risk Assessment

Formal risk assessments are conducted annually and when significant changes occur to systems or business processes. Risk assessment methodology follows ISO 27005 guidelines. Identified risks are tracked in a centralized risk register with assigned ownership, treatment plans, and target dates. Executive leadership reviews high and critical risks quarterly.

10.5 Vulnerability Management

Automated vulnerability scanning occurs weekly for all systems. Critical vulnerabilities are remediated within 48 hours, high within 7 days, medium within 30 days, and low within 90 days. Patch management follows vendor security advisories with emergency patching procedures for zero-day vulnerabilities.

Appendix A: Contact Information

Department	Contact	Availability
Security Operations Center	soc@cloudguard.tech +1-555-SEC-247/365	24/7/365
Security Incident Hotline	security@cloudguard.tech +1-555-URGENT	24/7/365
Compliance & Audit Requests	compliance@cloudguard.tech	Business hours
Privacy & Data Protection Office	privacy@cloudguard.tech	Business hours
General Security Inquiries	infosec@cloudguard.tech	Business hours

Appendix B: Document Revision History

Version	Date	Changes	Approved By
2.4	Dec 15, 2024	Updated certification dates, added ISO 27017/27018	CISO
2.3	Sep 10, 2024	Enhanced incident response procedures	CISO
2.2	Jun 5, 2024	Updated encryption standards to include TLS 1.3	Security Director
2.1	Mar 1, 2024	Added Singapore data center information	VP Infrastructure
2.0	Jan 1, 2024	Major revision - alignment with ISO 27001:2022	CISO

This document contains confidential and proprietary information of CloudGuard Technologies Inc. It is provided solely for the purpose of vendor security assessment and may not be reproduced or distributed without written authorization. For questions or clarifications regarding this documentation, please contact compliance@cloudguard.tech.