ENTERPRISE INFORMATION SECURITY POLICY MANUAL

Global Financial Services Corporation

Classification: INTERNAL USE ONLY

Document Version: 3.2.1

Effective Date: January 15, 2024

Last Updated: February 6, 2026

==========

SECTION 1: ACCESS CONTROL POLICIES

==========

1.1 Password Requirements

All employees must adhere to the following password standards:

Minimum password length: 12 characters for standard users, 16 characters for administrative accounts. Passwords must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

EXCEPTION: Legacy systems running on Windows Server 2012 R2 or older may use minimum 8-character passwords due to system limitations. These systems must be upgraded by December 31, 2025, OR isolated on a separate network segment with additional monitoring.

Password expiration: 90 days for standard accounts, 60 days for privileged accounts. However, NIST guidelines (SP 800-63B) recommend against forced password changes unless compromise is suspected. This creates a CONTRADICTION

with our current policy. Resolution: Risk assessment required by March 2026.

1.2 Multi-Factor Authentication (MFA)

MFA is MANDATORY for:

- All remote access (VPN, cloud services)

- Financial transaction systems

- Customer data repositories

MFA methods accepted: Hardware tokens (preferred), authenticator apps, SMS (only for non-critical systems due to SIM swap risks).

RISK ALERT: SMS-based MFA has been compromised in 47% of targeted attacks according to our 2024 security audit. Phase-out deadline: June 30, 2026.

==========

SECTION 2: DATA CLASSIFICATION AND HANDLING

==========

2.1 Data Classification Levels

Level 1 - PUBLIC: Marketing materials, published financial reports

Level 2 - INTERNAL: Memos, internal announcements, training materials

Level 3 - CONFIDENTIAL: Customer PII, employee records, financial forecasts

Level 4 - RESTRICTED: M&A data, security vulnerabilities, encryption keys

THRESHOLD: Any document containing >100 customer records automatically

qualifies as CONFIDENTIAL minimum, regardless of other content.

2.2 Data Retention Requirements

Customer transaction logs: 7 years (regulatory requirement - SEC Rule 17a-4)

Email communications: 3 years

System access logs: 1 year

Deleted file backups: 30 days then permanent deletion

EXCEPTION FOR LITIGATION HOLD: If litigation is anticipated or active, ALL relevant data must be preserved indefinitely until legal counsel confirms release. This overrides standard retention schedules.

CONTRADICTION: Section 2.2 states 30-day deletion for backups, but Section 8.3 (Disaster Recovery) requires 90-day backup retention for system restoration purposes. Resolution: Legal hold takes precedence; technical teams must maintain separate litigation backup sets.

==========

SECTION 3: INCIDENT RESPONSE PROCEDURES

==========

3.1 Severity Classification

SEV-1 (Critical): Data breach >1000 records, ransomware attack, system-wide outage affecting >50% of users. Response time: 15 minutes. Escalate to CISO immediately.

SEV-2 (High): Data breach <1000 records, targeted phishing campaign, unauthorized access to sensitive systems. Response time: 1 hour.

SEV-3 (Medium): Malware infection contained to single endpoint, policy violation without data exposure. Response time: 4 hours.

SEV-4 (Low): Spam reports, minor policy violations. Response time: 24 hours.

3.2 Communication Protocols

Internal notification: Security team within 15 minutes of detection.
Regulatory notification: Within 72 hours of breach confirmation (GDPR requirement) or "without unreasonable delay" (state laws vary).

RISK: California requires notification if >500 residents affected. Texas requires notification for any breach. New York SHIELD Act has different thresholds. Compliance matrix must be checked for each incident.

==========

SECTION 4: THIRD-PARTY RISK MANAGEMENT

==========

4.1 Vendor Classification

Critical vendors: Have direct access to production systems or >10,000 customer records. Require annual security assessments and SOC 2 Type II reports.

Standard vendors: Limited access, <10,000 records. Require self-assessment questionnaire and evidence of cyber insurance ($5M minimum).

4.2 Contract Requirements

All vendor contracts MUST include:

- Right to audit clause
- Data breach notification within 24 hours
- Data deletion certification upon termination
- Prohibition on subcontracting without written approval

EXCEPTION: Emergency vendors (disaster recovery services) may operate under master service agreements with modified terms, provided legal review is completed within 30 days of engagement.

==========

SECTION 5: CLOUD SECURITY STANDARDS

==========

5.1 Approved Cloud Providers

Primary: AWS (GovCloud for sensitive workloads), Azure

Secondary: Google Cloud Platform (development only)

Prohibited: Consumer-grade services (Dropbox personal, Google Drive personal)

5.2 Data Sovereignty Requirements

EU customer data: Must remain in EU regions (GDPR Article 44)

US government data: FedRAMP authorized environments only

Healthcare data: HIPAA-compliant environments with BAA in place

CONTRADICTION: Marketing team uses Salesforce which stores data globally. Exception granted via Data Processing Agreement, but this conflicts with strict data localization requirements in Germany and France. Resolution: Geofencing implemented for EU instances; review required Q2 2026.

==========

SECTION 6: REMOTE WORK SECURITY

==========

6.1 Endpoint Requirements

All remote devices must have:

- Full disk encryption (BitLocker for Windows, FileVault for Mac)
- EDR (Endpoint Detection and Response) agent installed
- Automatic screen lock after 5 minutes of inactivity
- Company-managed antivirus (CrowdStrike Falcon)

THRESHOLD: Devices with access to RESTRICTED data must use hardware security keys for authentication. No exceptions permitted.

6.2 Network Security

Home WiFi: WPA3 encryption required. WPA2 acceptable until December 2026.
Public WiFi: Prohibited for accessing CONFIDENTIAL or higher data. Use corporate VPN only.

RISK ASSESSMENT: 23% of remote workers admit to accessing work data from personal devices. This violates policy but enforcement is technically challenging. Enhanced DLP (Data Loss Prevention) controls deployed Q1 2026.

==========

SECTION 7: PRIVACY REQUIREMENTS

==========

7.1 Data Subject Rights (GDPR/CCPA)

Right to Access: Response within 30 days
Right to Deletion: Response within 45 days (with exceptions for legal holds)
Right to Portability: Data provided in machine-readable format (JSON/CSV)

7.2 Consent Management

Explicit consent required for:
- Marketing communications (opt-in only, no pre-checked boxes)
- Data sharing with third parties
- Automated decision-making with legal/significant effects

EXCEPTION: "Legitimate interest" may apply for fraud prevention and security monitoring, but legal review required before relying on this basis.

==========

SECTION 8: BUSINESS CONTINUITY AND DISASTER RECOVERY

==========

8.1 Recovery Time Objectives (RTO)

Critical systems (trading platforms): 4 hours

Important systems (email, CRM): 24 hours

Standard systems (HR portal): 72 hours

8.2 Recovery Point Objectives (RPO)

----------nCritical data: Zero data loss (synchronous replication)

Important data: 1 hour maximum loss

Standard data: 24 hours maximum loss

8.3 Backup Requirements

3-2-1 Backup strategy: 3 copies, 2 different media, 1 offsite

Backup testing: Quarterly restoration drills required

Retention: 90 days for operational recovery (SEE CONTRADICTION in Section 2.2)

==========

SECTION 9: SECURITY AWARENESS TRAINING

==========

9.1 Training Requirements

All employees: Annual security awareness training

Developers: Annual secure coding training + quarterly code reviews

Executives: Quarterly threat briefing sessions

IT Administrators: Annual certification (CISSP, CISM, or equivalent)

9.2 Phishing Simulation

Monthly phishing tests conducted. Failure rate threshold: <5%.

If department failure rate exceeds 10%, mandatory remedial training required.

==========

SECTION 10: COMPLIANCE AND AUDITING

==========

10.1 Regulatory Frameworks

SOX (Sarbanes-Oxley): Financial reporting controls

GDPR: EU data protection

CCPA/CPRA: California privacy rights

HIPAA: Health information (for employee benefits data)

PCI-DSS: Payment card data (if applicable)

10.2 Internal Audit Schedule

Comprehensive security audit: Annual

Penetration testing: Quarterly (external), continuous (automated)

Policy review: Bi-annual

Access certification: Quarterly manager attestation

RISK: Audit findings rated "High" or "Critical" must be remediated within 30 days. Extension requires CISO and Legal approval with documented risk acceptance.

==

APPENDIX A: EXCEPTION REQUEST PROCEDURE

==

To request a policy exception:

1. Submit formal request to security@gfs.com

2. Include business justification and risk assessment

3. Specify duration (temporary exceptions only, max 1 year)

4. Obtain approval from: Requester's VP + CISO + Legal (for CONFIDENTIAL+)

All exceptions are logged in the GRC (Governance, Risk, Compliance) system and reviewed quarterly by the Risk Committee.

==

APPENDIX B: CONTACT INFORMATION

==

Chief Information Security Officer (CISO): Sarah Chen (schen@gfs.com)

Security Operations Center (SOC): soc@gfs.com | +1-555-SEC-HELP

Privacy Officer: Michael Rodriguez (mrodriguez@gfs.com)

Compliance Hotline: 1-800-ETHICS-1 (anonymous reporting)

Document Owner: Information Security Department

Next Review Date: August 6, 2026