Centraline

Built Beyond Basics

Security Policy

INTRODUCTION AND SCOPE

This Security Policy establishes the framework for protecting information assets and technology infrastructure across all Centraline IT Services operations. The policy applies to all systems, data, facilities, and individuals engaged in the delivery of Centraline services, including but not limited to Managed IT Services, Ad-Hoc IT Services, Service Level Managed Support, website development, and hosting services. This comprehensive approach to security governance ensures consistent implementation of controls and safeguards throughout all service delivery activities and business operations, protecting both Centraline and client interests in accordance with applicable regulations and industry standards.

Centraline IT Services recognises that information security is integral to maintaining client trust and delivering reliable services. The objective of this Security Policy is to establish systematic protection against current and evolving threats while ensuring business continuity and minimising business risk. This document outlines our commitment to security excellence and defines the controls implemented across our technology landscape and service delivery framework.

SECURITY GOVERNANCE

Security governance at Centraline IT Services follows a risk-based approach that aligns security measures with business objectives and compliance requirements. The governance framework establishes accountability for security decisions, resource allocation, and policy enforcement through clearly defined roles and responsibilities. Authority for security governance resides with executive leadership, who review this policy annually and in response to significant operational or technological changes.

Security governance incorporates regular risk assessments, compliance monitoring, and performance measurement through security metrics. Security considerations are embedded in all business decisions, service delivery models, and technology implementations through established approval processes and security reviews. This approach ensures that security controls remain effective and proportionate to evolving threats and business requirements.

Centraline maintains a documented set of security standards and procedures derived from this policy, which provide detailed implementation guidance for technical controls and operational practices. These standards incorporate industry best practices from frameworks such as ISO 27001, NIST Cybersecurity Framework, and CIS Controls, adapted to our specific operational context and client requirements.

ACCESS CONTROL AND IDENTITY MANAGEMENT

Access to systems and data follows the principle of least privilege, providing only the minimum access rights necessary for individuals to perform their designated functions. All access requests undergo formal approval processes with appropriate segregation of duties. Authentication mechanisms implement multiple factors proportionate to the sensitivity of the assets being protected, with privileged access requiring enhanced verification measures.

Identity lifecycle management ensures timely provisioning and deprovisioning of access rights aligned with personnel status changes. Centraline implements just-in-time and just-enough access provision for privileged operations, with elevated access rights granted on a temporary basis and subject to additional monitoring. Regular access reviews validate the continued appropriateness of granted permissions, with any anomalies triggering immediate investigation.

Remote access to internal systems requires secure VPN connections with strong authentication enforcement. Client systems access follows client-approved protocols and security requirements, with all remote sessions monitored and logged for security purposes. Automated monitoring systems identify and alert on unusual access patterns or potential security violations, enabling rapid response to potential compromise attempts.

REMOTE SYSTEM CONNECTIVITY GOVERNANCE

Remote connectivity governance establishes secure methods for accessing, managing, and supporting both internal and client systems. All remote connections utilise encrypted transport protocols with mutual authentication and are subject to session timeouts after defined periods of inactivity. Remote management interfaces are never exposed directly to the internet and require multiple layers of access controls before establishing connection.

Secure remote access architecture implements an array of methods including network segmentation to prevent direct connectivity between internet-facing systems and sensitive backend resources. Remote support tools undergo security assessment before approval and implement granular permission controls, with client consent required before any remote session initiation. All remote support sessions are recorded with appropriate notifications provided to the recipients.

Centraline implements network-level controls including next-generation firewalls, intrusion detection/prevention systems, and secure web gateways to protect remote connectivity pathways. Remote access logs are centrally collected and analysed for security anomalies, with automated alerting for connection attempts outside established parameters. Regular security testing validates the effectiveness of remote access controls, with findings addressed through defined remediation processes.

DATA PROTECTION AND CLASSIFICATION

Centraline implements a comprehensive approach to data protection based on classification levels that determine appropriate security controls. All data is classified according to sensitivity and regulatory requirements, with controls applied consistently across all storage locations and processing environments. Encryption is implemented for data at rest and in transit according to classification levels and regulatory requirements.

Client data remains segregated through logical or physical means to prevent unauthorised access or cross-contamination. Data handling procedures define appropriate methods for the storage, processing, transfer, and disposal of information according to classification level. Data loss prevention technologies monitor for unauthorised data transfers or policy violations, with alerts generated for potential data protection incidents.

Data retention and disposal follow documented schedules aligned with legal, regulatory, and contractual requirements. Secure disposal processes ensure complete and irreversible destruction of confidential information when retention periods expire. Regular data protection audits verify compliance with established policies and identify potential vulnerabilities in data handling practices for remediation.

SYSTEM SECURITY AND HARDENING

System security begins with baseline security configurations developed for all technology platforms according to industry best practices and security benchmarks. All systems undergo hardening procedures before deployment, with unnecessary services, default accounts, and sample applications removed or disabled. System configuration standards specify required security settings, patch levels, and approved software components.

Change management processes govern all modifications to production systems, with security impact assessments conducted for significant changes. System patching follows defined schedules based on vulnerability severity, with critical security updates expedited through accelerated deployment processes. Systems undergo regular vulnerability assessments with findings addressed according to defined remediation timeframes.

Centraline maintains separate environments for development, testing, and production with appropriate access segregation to prevent unauthorised changes. Anti-malware protection is deployed across all applicable systems with current signature databases and behaviour-based detection capabilities. Host-based firewalls and intrusion prevention provide additional protective layers for critical systems and sensitive data repositories.

NETWORK SECURITY ARCHITECTURE

Network security implements defence-in-depth strategies with multiple control layers protecting critical assets. Network segmentation separates systems by security requirements and function, with controlled interfaces between segments. Perimeter security incorporates next-generation firewalls, intrusion detection/prevention systems, and web application firewalls to detect and block malicious traffic.

Internal networks utilise micro-segmentation where appropriate to limit lateral movement in the event of compromise. All network traffic between security zones is explicitly permitted through access control lists, with default deny policies for undefined traffic.

Network monitoring provides visibility into traffic patterns and security events, with automated alerts for suspicious activities. Regular network security assessments identify potential vulnerabilities, misconfigurations, or unauthorised connectivity. Network documentation is maintained with current diagrams, IP addressing schemes, and security control inventories to support incident response and security operations.

SECURITY MONITORING AND INCIDENT RESPONSE

Security monitoring establishes continuous visibility across systems, networks, and applications to detect potential security incidents. Log collection aggregates security-relevant events from all critical systems to enable correlation and analysis. Monitoring systems generate alerts based on defined thresholds and anomaly detection, with escalation procedures for various severity levels.

The incident response process defines a structured approach for addressing security incidents through preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. Incident classification determines appropriate response procedures and communication plans based on impact and scope. Containment strategies are defined for various incident types to limit damage and preserve evidence.

Investigation procedures establish systematic methods for determining incident scope, impact, and root cause. Response activities are documented throughout the incident lifecycle to support analysis and future improvements. Post-incident reviews identify lessons learned and control improvements to reduce future risk. When required by regulation or contract, incidents are reported to affected parties and authorities within defined timeframes.

VULNERABILITY MANAGEMENT

Vulnerability management implements a systematic approach to identifying, assessing, and remediating security weaknesses across all technology assets. Vulnerability scanning is conducted regularly against internal and external systems with appropriate authorisation and scope limitations. Remediation priorities are assigned based on vulnerability severity, affected asset criticality, and exploitation potential.

Discovered vulnerabilities are tracked through defined workflows from identification to resolution, with status reporting and escalation for overdue items. High-risk vulnerability findings receive expedited treatment with compensating controls implemented when immediate patching is not feasible. Special attention is given to public-facing systems and applications processing sensitive data.

Penetration testing is conducted periodically by qualified security professionals to identify vulnerabilities requiring sophisticated exploitation techniques. Security testing results are reviewed with findings prioritised for remediation according to risk. Vulnerability intelligence sources are monitored for emerging threats requiring rapid response or out-of-cycle patching activities.

SUPPLIER SECURITY MANAGEMENT

Centraline recognises that suppliers and service providers form an extension of our operational environment with potential security implications. Security requirements are defined in contracts and service level agreements according to the level of access and data handling involved. Suppliers with access to sensitive data or systems undergo security assessment before engagement and periodically thereafter.

Supplier access to Centraline systems follows the same security principles applied to internal access, including least privilege and strong authentication. Third-party services and products undergo security evaluation before approval, with particular attention to data protection capabilities and security track record. Supplier security incidents affecting Centraline or client data require immediate notification as specified in contractual terms.

Cloud service providers are selected with consideration of security capabilities, compliance certifications, and data sovereignty requirements. Centraline maintains oversight of outsourced security functions through regular reviews, performance measurement, and independent validation. Supplier relationships involving critical functions or sensitive data receive enhanced scrutiny and ongoing monitoring.

PHYSICAL AND ENVIRONMENTAL SECURITY

Physical security controls protect facilities, equipment, and information assets from unauthorised access and environmental threats. Access to facilities requires authentication, with visitor management procedures controlling non-employee entry. Sensitive areas implement additional access controls proportionate to the assets being protected. Physical access rights undergo regular review and prompt adjustment when personnel changes occur.

Environmental controls protect technology assets from power failures, temperature extremes, water damage, and fire. Critical infrastructure receives appropriate redundancy and monitoring to ensure continued operation. Equipment maintenance follows manufacturer recommendations with appropriate security considerations for repair activities. Asset management tracks the location and status of technology components throughout the lifecycle.

Physical media handling includes secure storage, controlled access, and appropriate disposal methods based on data sensitivity. Secure disposal processes ensure data cannot be recovered from decommissioned equipment or media. Regular inspections verify the continued effectiveness of physical and environmental controls, with deficiencies addressed through defined remediation processes.

APPLICATION SECURITY AND SECURE DEVELOPMENT

Application security begins with secure development practices integrated throughout the software development lifecycle. Security requirements are defined during the initial planning phase and validated through appropriate testing before production deployment. Secure coding standards provide developers with guidance on preventing common vulnerabilities and implementing robust security controls.

Application security testing includes static code analysis, dynamic testing, and manual security review proportionate to application criticality and risk. Third-party code, libraries, and components are evaluated for security vulnerabilities before incorporation into applications. Security defects are tracked with the same priority as functional defects, with critical vulnerabilities addressed before production release.

Web applications implement appropriate security controls including input validation, output encoding, authentication, session management, and access control. API security includes robust authentication, rate limiting, and input validation with security testing specific to API attack vectors. Applications handling sensitive data implement appropriate encryption with secure key management practices.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity planning ensures the continued operation of critical services during disruptive incidents. Business impact analysis identifies essential functions, maximum acceptable downtime, and recovery priorities. Continuity strategies define alternate processing methods, staffing approaches, and communication plans for various disruption scenarios.

Disaster recovery planning focuses on the restoration of technology systems and data following significant disruption. Recovery point objectives and recovery time objectives are defined according to business requirements and criticality. Backup strategies implement appropriate frequency, retention, and verification based on data importance and change rates.

Backup systems receive appropriate security controls to prevent unauthorised access or modification of recovery data. Recovery capabilities undergo regular testing to validate effectiveness and identify improvements. Incident response and business continuity plans are coordinated to ensure comprehensive coverage of security incidents with business impact potential.

COMPLIANCE AND RISK MANAGEMENT

Compliance management ensures adherence to applicable laws, regulations, contractual obligations, and internal policies. Regular compliance assessments identify gaps requiring remediation, with findings tracked through resolution. Changes to the regulatory environment are monitored with timely updates to affected controls and practices.

Risk management provides a structured approach to identifying, assessing, and addressing security risks across the organisation. Risk assessments evaluate threats, vulnerabilities, impacts, and existing controls to determine risk levels and appropriate responses. Risk treatment decisions consider risk acceptance, mitigation, transfer, or avoidance based on defined tolerance thresholds.

Security metrics provide ongoing visibility into the effectiveness of the security program, with regular reporting to appropriate stakeholders. Internal audits verify control effectiveness and policy compliance, with findings addressed through formal remediation processes. The security policy framework undergoes regular review and update to maintain alignment with current threats, technology changes, and business requirements.

AWARENESS AND TRAINING

Security awareness establishes a culture of security consciousness throughout the organisation. Awareness activities communicate security responsibilities, current threats, and expected behaviours through various channels. All personnel receive security orientation during onboarding and ongoing awareness updates addressing evolving threats and lessons learned.

Role-based security training provides specialised knowledge for individuals with specific security responsibilities. Technical personnel receive training appropriate to their roles in maintaining secure systems and responding to security incidents. Personnel with access to sensitive data receive additional training on data protection requirements and handling procedures.

Awareness effectiveness is measured through various mechanisms including simulated phishing exercises, knowledge assessments, and behaviour observation. Security culture is reinforced through recognition of positive security practices and constructive follow-up for security policy violations. Training content is updated regularly to address emerging threats and changes to security requirements.

CLIENT SYSTEM SECURITY MANAGEMENT

Client system security management establishes consistent security practices for systems under Centraline management or support. Security baselines are implemented according to industry standards, client requirements, and assessed risk levels. System monitoring provides visibility into security status, performance metrics, and potential issues requiring attention.

Security patch management follows defined schedules with appropriate testing and approval processes. System configuration is managed through documented procedures with change control and validation testing. Security assessments identify vulnerabilities and compliance gaps requiring remediation through established workflows.

Client security documentation is maintained with current system information, configuration details, and security control inventories. Security incidents affecting client systems follow defined response procedures with appropriate client notification and coordination. Security recommendations are provided to clients based on observed vulnerabilities, emerging threats, and best practice developments.

CRYPTOGRAPHY AND KEY MANAGEMENT

Cryptographic controls protect the confidentiality and integrity of sensitive information throughout its lifecycle. Encryption algorithms and key lengths follow current industry standards and best practices, with deprecated algorithms phased out according to defined schedules. Encryption is implemented for sensitive data at rest, in transit, and where required by regulation or contract.

Cryptographic key management establishes secure processes for key generation, distribution, storage, rotation, and destruction. Key access follows least privilege principles with appropriate segregation of duties. Critical keys receive enhanced protection through hardware security modules or equivalent strong protection mechanisms.

Certificate management ensures timely renewal of security certificates with appropriate validation of certificate requests. Private keys receive protection commensurate with the sensitivity of the information they secure. Cryptographic implementations undergo periodic review to ensure continued alignment with current standards and best practices.

This Security Policy demonstrates Centraline IT Services' commitment to protecting both internal and client information assets through a comprehensive and systematic approach to security. The controls and practices defined in this policy are designed to address current threats while maintaining the flexibility to adapt to the evolving security landscape. Regular review and continuous improvement ensure that our security posture remains effective against emerging risks.

Security at Centraline is not merely a set of technical controls but a fundamental aspect of our service delivery approach and business operations. By implementing the principles and practices outlined in this policy, Centraline provides clients with confidence that their systems and data receive appropriate protection throughout the service relationship. Security is embedded in everything we do, from initial client engagement through ongoing service delivery and support.

The policies and procedures referenced in this document are available to personnel through our internal policy repository, with appropriate information provided to clients regarding security practices relevant to their services.

Centraline
Built Beyond Basics

Security Policy

Centraline IT Services

International House, 10 Churchill Way, Cardiff, CF10 2HE, United Kingdom

Last updated: 27th April 2025