



Centralpoint & Oxcyon Data Protection Process

Data Leakage Prevention Controls and Process

1.0 Purpose

Protection against inappropriate data leaks — data leakage prevention (DLP) is a critical part of Oxcyon's internal processes, applied consistently across Oxcyon and its technology partners as part of the overall Information Security program. Data leaks can occur through accidental sharing of sensitive information, malicious action by insiders or external attackers, or vulnerabilities in software and systems. This document sets out the controls Oxcyon has implemented to prevent them.

2.0 Scope

This process applies to all data Oxcyon and Centralpoint collect, process, store, or transmit on behalf of the business or its clients, and to every employee, contractor, and technology partner with access to that data. It operates alongside the Oxcyon Information Security Policy and Oxcyon Access Policy, which govern the underlying access, classification, and confidentiality requirements this process implements day to day.

3.0 Data Protection Controls

3.1 Data Classification

Data is classified based on its sensitivity, which determines the level of protection it receives — personal, financial, or health data is classified as highly sensitive, while public information requires less protection. This follows the Confidential / Internal / Public classification scheme defined in the Oxcyon Information Security Policy.

3.2 Data Inventory

Oxcyon maintains an inventory of the data it collects, processes, and stores. Knowing where data resides is a prerequisite for protecting it effectively, and this inventory is what the classification scheme in Section 3.1 is applied against.

3.3 Access Control

Strict access controls ensure only authorized personnel can reach sensitive data, using role-based access control (RBAC) and the principle of least privilege so access is limited to what an employee needs to do their job. Full access provisioning, MFA, and offboarding requirements are defined in the Oxcyon Access Policy.

3.4 Encryption

Centralpoint's Microsoft SQL Server 2019 databases use Transparent Data Encryption (TDE) to protect data at rest — encrypting database files, backups, and transaction logs so they are unreadable without the encryption key, even if the underlying storage is compromised. Data in transit is separately protected with TLS. Together these protect sensitive data whether it is moving in and out of Centralpoint or sitting at rest inside it. See the SQL 2019 TDE Encryption and Database Restore Procedure for the technical implementation:

3.5 User Education and Awareness

Oxcyon trains employees in data security best practices, including how to recognize and respond to phishing attacks, social engineering attempts, and other tactics that lead to data leaks. This training is reinforced by the acceptable-use rules in the Oxcyon Access Policy.

3.6 Data Loss Prevention (DLP) Solutions

DLP tooling monitors and enforces data security policy, identifying and blocking unauthorized data transfers whether intentional or accidental. Rackspace, as Oxcyon's hosting partner, provides this monitoring for externally facing traffic — see Section 3.15, Vendor Risk Management, for how that arrangement is governed.

3.7 Data Masking and Anonymization

When sharing data with third parties or using it for testing, Oxcyon applies data masking or anonymization to protect sensitive information while still allowing the necessary access.

3.8 Network Segmentation

Segmentation within Oxcyon's networks limits the flow of sensitive data and creates barriers that prevent unauthorized access or lateral movement by an attacker, consistent with the Development, QC, and Production environment separation described in the Centralpoint System Requirements documentation.

3.9 Logging and Monitoring

Logging and monitoring systems detect suspicious activity or access to sensitive data. Logs are reviewed regularly for signs of data leaks or security breaches, and any confirmed finding is handled per Section 3.10.

3.10 Incident Response

A suspected data leak or breach is handled under the Incident Response Plan, which defines containment, investigation, notification, and recovery steps, and the Incident Flowchart, which shows the triage decision path at a glance.

3.11 Regular Auditing and Assessments

Regular security audits and assessments identify vulnerabilities and weaknesses in Oxcyon's data protection measures, with findings addressed promptly and tracked to closure.

3.12 Compliance with Regulations

Oxcyon's data protection practices are designed to comply with the regulations relevant to each client's industry and location, which may include GDPR, HIPAA, or PCI DSS. Where EU residents' personal data is involved.

3.13 Data Retention and Disposal

Oxcyon retains data only for as long as it serves the purpose it was collected for, and disposes of it securely once that purpose has been met, reducing the risk of a leak from outdated or unnecessary information. See Assumptions for confirmation of the specific retention schedules by data type.

3.14 Remote Work Security

Oxcyon supports remote work through a range of tools, with remote access secured by VPN, multi-factor authentication, and approved collaboration tools, per the remote access requirements in the Oxcyon Access Policy.

3.15 Vendor Risk Management

Oxcyon assesses the security practices of third-party vendors and partners with access to its data, including hosting partners such as Rackspace, to confirm they maintain robust security measures. This follows the third-party risk process described in the Oxcyon Information Security Policy and the Centralpoint Web API Security Policy.

4.0 Ongoing Nature of This Process

Protection against inappropriate data leaks is an ongoing process that requires a combination of technology, policy, and employee awareness. Oxcyon adapts and evolves this process as new threats and technologies emerge, reviewing it on the cadence set in Document Control.

Change Tracking and Scope Control

All tasks and any changes to the implementation scope are logged in Oxcyon's issue management system and tagged to the assigned Production Manager. This gives every change a full audit trail, keeps the work monitored and accountable, and controls scope creep. The system is available at <https://oxcyoninc.aceproject.com>

Glossary of Terms

DLP (Data Loss Prevention) Tooling and process controls that identify and block unauthorized transfer of sensitive data, whether intentional or accidental.

Data Masking / Anonymization — Techniques that obscure or remove identifying details from data so it can be shared or tested with while protecting the underlying sensitive information.

Least Privilege — Granting a user only the access their role requires, rather than broad access by default.

Network Segmentation— Dividing a network into separate zones to limit how far an attacker or a data leak can spread.

RBAC (Role-Based Access Control) — An access model that grants permissions based on a user's role rather than to individuals directly.

TDE (Transparent Data Encryption) A SQL Server feature that encrypts database files, backups, and transaction logs at rest.

TLS (Transport Layer Security) The cryptographic protocol used to encrypt data in transit between two systems.