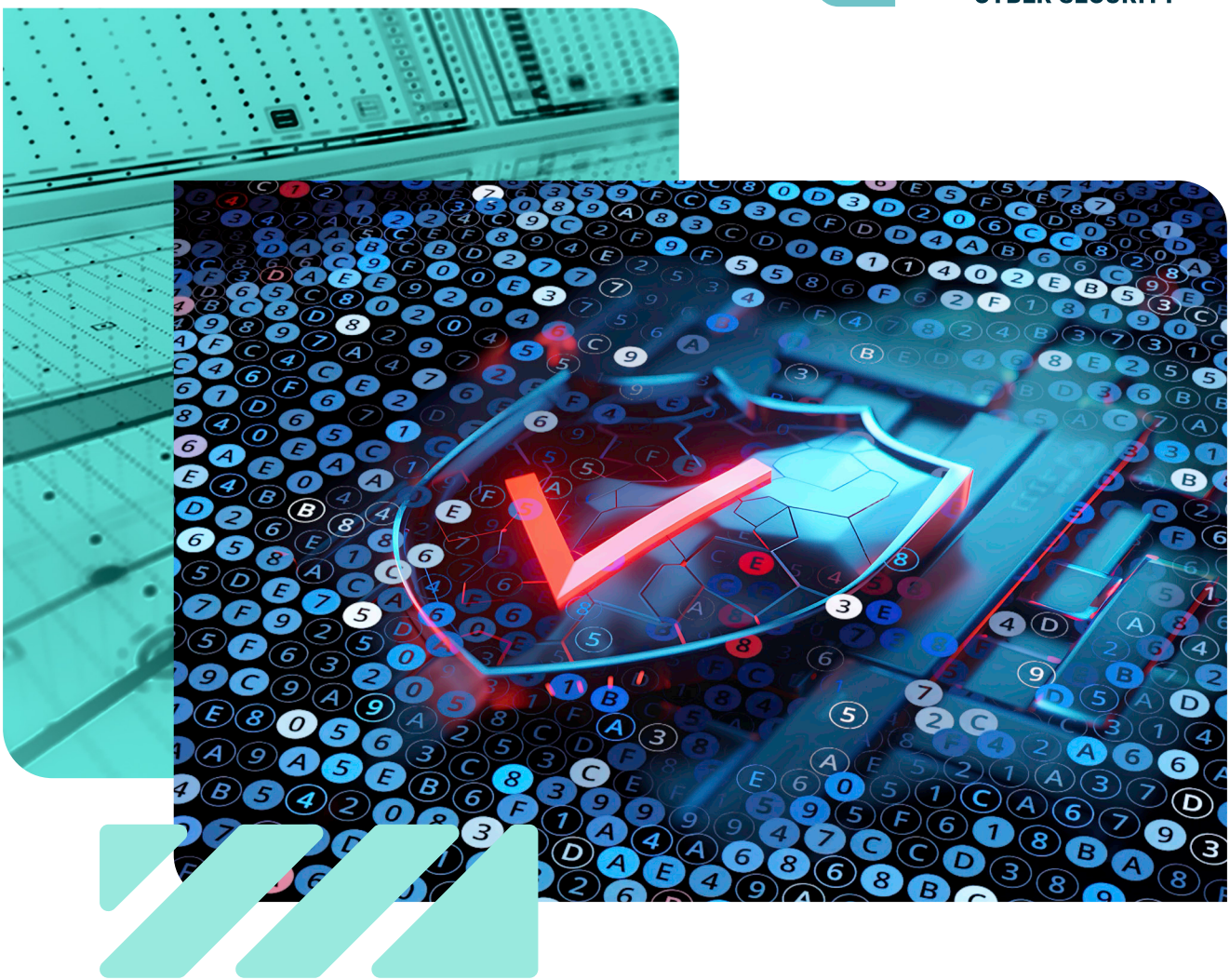
NORTHWAVE
CYBER SECURITY



Data Security
Essential Implementation

Take control of your sensitive data

As your organisation's data estate expands and digital risks evolve, protecting sensitive information is no longer optional. Take charge of your data with aligned policies, secure technologies, and aware employees.

From insight to action

Northwave's Data Security Essential Implementation helps you move from insight to action, building on the results of your Data Security Workshop to establish practical, sustainable improvements across your business, technology, and employee behaviour.

Key benefits:

- **Gain control over your sensitive data.**
- **Meet compliance and supply chain requirements with confidence.**
- **Embed data protection into your organisational culture.**
- **Prepare for future security enhancements with a scalable foundation.**
- **Benefit from our integrated approach: Business, Bytes & Behaviour.**

Our approach

Northwave's Data Security Essential Implementation follows a structured, fixed-price approach that connects strategy with real-world execution. We work side by side with your team to ensure every layer of your organisation, business processes, technology, and employee behaviour, aligns with your data protection goals.

From configuration to confidence

Our implementation journey combines clear governance, technical configuration, and behavioural alignment to make your data security strategy work in practice.

Step 1: Define policies and objectives
- We help you translate business requirements and compliance needs into clear, actionable data security policies.

Step 2: Assign roles and responsibilities
- Together, we establish ownership, ensuring your team knows who manages, monitors, and enforces data protection.

Step 3: Classify & label data
- Using Microsoft Purview, we implement sensitivity labels and classification rules that match your organisation's context.

Step 4: Configure Microsoft Purview
- Our experts set up Data Loss Prevention (DLP), retention, and insider risk configurations tailored to your environment.

Validation through simulation

Once configured, we run a three-week simulation period to test your setup in realistic conditions, verifying its effectiveness without disrupting daily operations.

At the end, you'll receive a comprehensive report with:
- Policy improvement recommendations
- Technical optimisation advice
- Behavioural training suggestions

This ensures your organisation doesn't just deploy data protection technology, it builds confidence, control, and culture around data security.

What's included

The Data Security Essential Implementation provides the building blocks for sustainable data protection, helping you take control of your sensitive information and meet compliance expectations. Our modular approach ensures every organisation can tailor the implementation to its needs, from foundational protection to advanced integrations.

By default, the implementation focuses on your Microsoft 365 environment, covering Exchange Online, SharePoint Online, and Microsoft Teams. This ensures a strong and consistent foundation within your core collaboration and communication platforms. If desired, the scope can be expanded to include supported Windows endpoints, on-premises data sources, and custom applications, extending data protection to your full digital ecosystem.

Standard modules (core capabilities)

Data Loss Prevention (DLP)
- Establish consistent data protection rules across your Microsoft 365 environment. This module includes the configuration of sensitivity labels, data retention labels, and Sensitive Information Types (SITs) to identify and protect critical data, wherever it resides or moves within your environment.

Insider Risk Management
- Detect and mitigate risky or unintended user behaviour before it leads to data loss or compliance breaches. Gain insight into internal data movement and apply privacy-aware controls to protect sensitive information.

Compliance Manager
- Simplify compliance management with automated assessments and built-in recommendations. Track progress against regulations and frameworks, and streamline evidence collection and audit readiness.

eDiscovery
- Enable secure and efficient data search, investigation, and export for legal or regulatory purposes. Respond confidently to information requests and investigations while maintaining data integrity and privacy.

Optional modules (advanced capabilities)

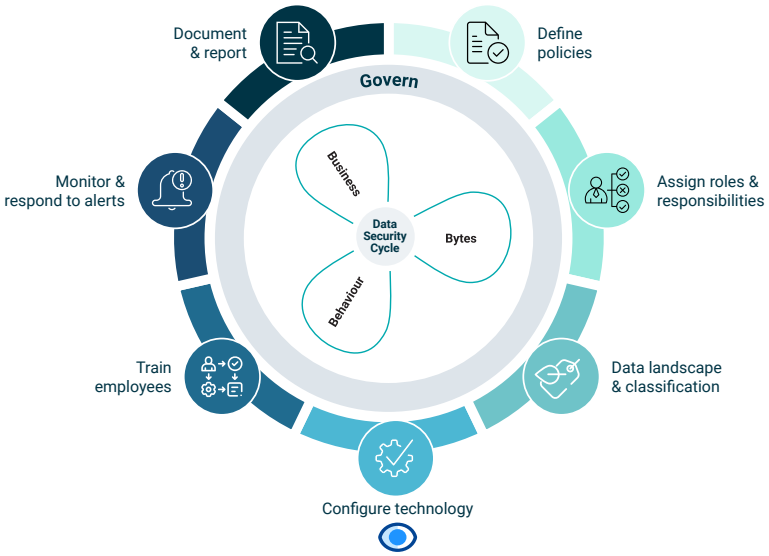
Data Security Posture Management (DSPM) for AI
- Extend visibility to data used in AI systems and cloud environments. Identify, classify, and protect sensitive data in AI-driven workflows to ensure responsible, compliant, and secure data use.

Communication Compliance
- Monitor and manage communication channels to detect and address potential data leaks, policy violations, or misconduct. This module supports responsible communication practices and strengthens your organisation's compliance posture.

The data security cycle

The Data Security Cycle is a practical framework developed by Northwave to help organisations establish, implement, and continuously improve data protection. It connects policy, technology, and people, ensuring that data security becomes an integrated and sustainable part of daily operations, not a one-off project.

Northwave uses this framework to guide clients through each stage of their data protection journey, helping them build lasting control and confidence in how sensitive information is managed.



Define policies

Establish clear, actionable data protection policies aligned with your organisation's objectives, regulatory obligations, and risk landscape. These policies form the foundation for consistent and compliant data management.

With the Essential Implementation, we help you establish clear, effective data protection policies tailored to your organisation's needs, regulatory obligations, and risk appetite. These policies form the backbone of your data governance framework.

Assign roles & responsibilities

Clarify ownership and accountability across departments. Effective data protection depends on every role, from leadership to individual employees, understanding their part in keeping information secure.

We guide you in allocating responsibilities across departments and functions, ensuring everyone, from management to end users, understands their role in protecting sensitive information.

Data landscape & classification

Gain visibility into where sensitive data resides, how it flows through your organisation, and who has access to it. Classify data according to sensitivity and business value, laying the groundwork for protection, retention, and monitoring measures. This step turns abstract policies into actionable insights and enables effective configuration later in the cycle.

During the implementation, Northwave supports your organisation in mapping data locations, identifying high-risk areas, and designing a classification model that aligns with your policies and operational reality. This ensures your technical configuration in Microsoft Purview is based on a clear understanding of your actual data landscape.

Configure technology

Implement and align technical controls with your defined policies. Platforms like Microsoft Purview enable classification, protection, and monitoring of data across the organisation, supporting enforcement of your security standards.

Our certified professionals configure Microsoft Purview to align with your defined policies and business processes. We ensure the technical foundation is robust, compliant, and ready to support your data security objectives.

Train employees

Raise awareness and build competence. Targeted training and communication help employees recognise sensitive information, follow security policies, and make responsible decisions in their daily work.

Our behavioural training team can provide focused awareness sessions that help employees recognise, handle, and protect sensitive data responsibly, turning awareness into daily practice.

Monitor & respond to alerts

Continuously monitor data activity to detect and respond to risks. Proactive detection, analysis, and response capabilities strengthen resilience and limit potential impact.

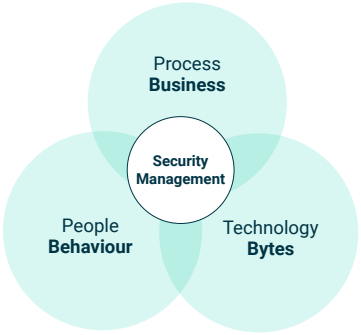
We're currently developing a monitoring and response service that proactively tracks data security alerts and supports timely response actions. If you're interested in exploring this capability alongside your implementation, we'd be happy to discuss what's already possible today.

Document & report

Maintain thorough documentation of your policies, activities, and incidents to demonstrate compliance and enable ongoing improvement. Transparent reporting supports internal governance and external accountability.

Your confident security crew

We provide 360° Intelligent Security Operations and unique solutions to specific challenges. Our approach is driven by intelligence, integrating business, bytes, and behaviour to protect your organisation. We are independent by nature and serve as a dedicated extension of your organisation, providing an expert view on every aspect of your cyber security.



By choosing our fully integrated services, you will benefit from improved security, increased time-efficiency and cost-effectiveness, as well as the convenience of working with fewer suppliers.

We are by your side

Ensuring the safety of your company while achieving your business goals is of utmost importance. We will gladly determine together with you what the best solution for your needs is.