HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

365 4 TOTAL PROTECTION & NIS2



How does 365 Total Protection help with NIS2 compliance?

As cyber threats continue to evolve, NIS2 is raising the bar for cybersecurity risk management across the European Union, with greater emphasis on governance, resilience, incident response, business continuity and employee awareness. Meeting these requirements calls for a comprehensive approach combining governance, technology, resilience and human awareness. **365 Total Protection can support organisations on this journey by providing security measures and compliance-related capabilities aligned with several NIS2 requirements.**

HORNETSECURITY BY proofpoint.

INFOSHEET AI POWERED

PROVISION	WHAT IT REQUIRES FOR THE CUSTOMER	HOW PRODUCTS CAN HELP	HOW 365 TOTAL PROTECTION HELPS	NIST PILLAR MAPPING	NIS2 DOMAIN
ARTICLE 20(1)	Management bodies must approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21 and oversee their implementation.	Governance dashboards, control approval workflows, board reporting, evidence packs.	Control Panel dashboards	Governance	Cybersecurity Risk Management
			365 Permission Manager dashboards and audit views		
			365 Total Backup backup/restore history & 4-eye approval		
			Security Awareness Service status and company certificate		
			Email Live Tracking		
			Audit logs		
ARTICLE 20(2)	Management bodies must complete cybersecurity training, and entities must offer similar training to employees.	Awareness training platforms, completion tracking, attestations, role-based training.	Security Awareness Service e-training modules, spear-phishing simulations, short videos, quizzes	Governance	Cybersecurity Risk Management
			SAS annual company certificate		
ARTICLE 21(1)	In-scope entities must take appropriate and proportionate technical, operational, and organisational measures to manage cybersecurity risk.	Core control platforms, risk management tooling, policy enforcement, evidence collection.	Combined control set across email security, encryption, continuity, backup, permissions governance, and awareness: Spam and Malware Protection, Content Control, Compliance Filter, Global S/MIME/PGP encryption, Websafe, Email Continuity Service, 365 Total Backup, 365 Permission Manager, Security Awareness Service, AI Recipient Validation, Teams Protection	Governance	Cybersecurity Risk Management
ARTICLE 21(2)(A)	Risk-analysis and information-system security policies.	Risk register tooling, policy lifecycle management, security control mapping.	Compliance Filter custom rules	Governance	Cybersecurity Risk Management
			365 Permission Manager compliance policies, automatic recurring re-audit of previously approved access, (upcoming) risk severity classification		
			Email Live Tracking		
			Audit logs		
			Dashboard views for compliance and backup status		

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

PROVISION	WHAT IT REQUIRES FOR THE CUSTOMER	HOW PRODUCTS CAN HELP	HOW 365 TOTAL PROTECTION HELPS	NIST PILLAR MAPPING	NIS2 DOMAIN
ARTICLE 21(2)(B)	Incident handling.	SIEM/SOAR, incident case management, playbooks, ticketing.	Integration with SIEM and SOARs, either native or via APIs Native alerting and Monitoring feature in CP.	Detect / Respond	Cybersecurity Risk Management
ARTICLE 21(2)(C)	Business continuity, including backup management, disaster recovery, and crisis management.	Backup orchestration, DR testing, continuity planning, crisis workflows.	Email Continuity Service 365 Total Backup	Recover	Cybersecurity Risk Management
ARTICLE 21(2)(D)	Supply-chain security, including security aspects of relationships with direct suppliers and service providers.	Third-party risk management, supplier questionnaires, continuous vendor monitoring.	365 Permission Manager external sharing controls, sharing-link detection and remediation, anomalous-permission detection AI Recipient Validationto avoid accidental data loss to a supplier or service provide Email encryptionto secure external communication with suppliers and service providers	Governance	Cybersecurity Risk Management
ARTICLE 21(2)(F)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	Control testing, continuous compliance, audit evidence, KPI/KRI dashboards.	365 Permission Manager compliance dashboards and activity log 365 Total Backup backup health, activity log and restore history Security Awareness Service ESI, statistics and annual certificate Email Live Tracking and other email statistics Audit logs	Governance	Cybersecurity Risk Management
ARTICLE 21(2)(G)	Basic cyber hygiene practices and cybersecurity training.	Security awareness, phishing simulation, hygiene baselines, endpoint posture checks.	Security Awareness Service e-training modules, spear-phishing simulations, short videos, quizzes SAS annual company certificate	Protect	Cybersecurity Risk Management
ARTICLE 21(2)(H)	Policies and procedures on cryptography and, where appropriate, encryption.	Key management, encryption policy enforcement, certificate lifecycle tooling.	Email encryption	Protect	Cybersecurity Risk Management

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

PROVISION	WHAT IT REQUIRES FOR THE CUSTOMER	HOW PRODUCTS CAN HELP	HOW 365 TOTAL PROTECTION HELPS	NIST PILLAR MAPPING	NIS2 DOMAIN
ARTICLE 21(2)(I)	Human resources security, access control policies, and asset management.	IAM, joiner-mover-leaver workflows, asset inventory, privileged access control.	365 Permission Manager permission reports, siteowner delegation, external-sharing levels, auto-remediation, activity log; email archive private/test-access controls	Protect	Cybersecurity Risk Management
			365 Total Backup bulk user management		
ARTICLE 21(2)(J)	MFA or continuous authentication, secured voice/video/text communications, and secured emergency communications, where appropriate.	MFA/SSO, conditional access, secure comms, emergency communications.	Email encryption	Protect	Cybersecurity Risk Management
			Websafe		
ARTICLE 23(2)	Notification without undue delay, with a 24- or 72-hour timeframe depending on the incident.	24-hour alerting, triage automation, initial classification, duty roster support.	Advanced Threat Protection real-time alerts and AutoRemediate	Respond	Information Sharing
			Email Live Tracking		
			AI Email Security Analyst helps to characterize an incident involving emails		
			365 Permission Manager automated remediations		

Strengthen your NIS2 cybersecurity strategy

NIS2 compliance requires an organisation-wide approach combining governance, processes, people and technology. No individual security product can establish compliance on its own.

365 Total Protection can contribute to that broader strategy by providing security, resilience, governance and awareness capabilities that help organisations address measures associated with key NIS2 requirements, from email security and encryption to backup, permissions management, incident visibility and security awareness.

Together, these capabilities can help organisations strengthen their cybersecurity posture and support their ongoing NIS2 compliance journey.

START YOUR FREE TRIAL NOW

Sources: European Commission policy page • European Commission NIS2 FAQ • Official NIS2 text on EUR-Lex