The EU Directive on Security of Network and Information Systems (NIS Directive)

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The NIS Directive applies primarily to Operators of Essentials Services (OES) that are identified by EU Member States and Digital Services Providers (DSP) that offer key digital services to persons within the EU. The NIS Directive entered into force in August 2016. EU member states – including the UK –were required to transpose the NIS Directive into their national laws by 9 May 2018 and must identify Operators of Essential Services by 9 November 2018.

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
		Objective A: Managing security risk	
A.2 Risk Management	**Segregation of duties** *Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets*	All Sophos products	Sophos' user-identity based policy technology allows user level controls over network resources and other organization's assets.
	Mobile device policy *A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices*	Sophos Mobile	Provides Enterprise Mobility and security management capabilities for mobile devices, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
	Teleworking Policy *A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites*	Sophos Firewall/UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		SafeGuard Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard encryption.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
A.3 Asset management	*Protect authorized endpoint and other devices connected to the network; including workstations, laptops, mobile devices, servers and remote devices; by effective monitoring and configuration management.*	Sophos Endpoint Protection Sophos Intercept X for Server	Enforces web, application and device policies for Windows, Mac and Linux systems; When used with Sophos XG Firewall it automatically detects and isolates malware infected endpoint devices from network resources.
		Sophos Mobile	Device management solution for smartphones, tablets etc. Enforces security policies and monitors device health. Automatic remediation assures safety of device and corporate data.
		Sophos XG Firewall with Security Heartbeat™	Allows next generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised/ unauthorized endpoint device, allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data to a C2 server; drastically improves incident response time.
A.4 Supply chain	**Network controls** *Networks shall be managed and controlled to protect information in systems and applications.*	XG Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
		Sophos Mobile	Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X and Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.

SOPHOS

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
	Information transfer policies and procedures *Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.*	Sophos Email Appliance	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Enterprise	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. SafeGuard manages BitLocker and FileVault full disk encryption, as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		XG Firewall	Allows for policy-based encryption for VPN tunnels, protecting data in transit.
	Electronic messaging *Information involved in electronic messaging shall be appropriately protected.*	Sophos Email Appliance	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace dynamically encrypts content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
		Sophos SafeGuard Enterprise	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. SafeGuard manages BitLocker and FileVault full disk encryption, as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
Objective B: Protecting against cyber attack			
B.1 Service protection policies and processes	**Termination and change of employment responsibilities** *There should be a process that ensures access to information assets are removed at the time of termination.*	Sophos Firewall/UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth and other network resources.
		Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
B.2 Identity and access control	**Access to network and network services** *Users shall only be provided with access to the network and network services that they have been specifically authorized to use.*	Sophos Firewall/UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		SafeGuard Enterprise	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
	Removal or adjustment of access rights *The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.*	Sophos Firewall/UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth and other network resources.
		Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Management of privileged access right *The allocation and use of privileged access rights shall be restricted and controlled.*	Sophos Enterprise Console and Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Mobile	Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Firewall Manager	Centralized security management with extensive administrative controls; Role-based administration with change control and logging.
B.3 Data security	**Effective data loss prevention capabilities** *Safeguard mission-critical data while preventing unauthorized access to sensitive information.*	Sophos Intercept X and Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		SafeGuard Enterprise	Complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as in transit.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Mobile	Delivers mobile data protection when integrated with SafeGuard Enterprise to enable access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separated from personal data and can be locked down or wiped.
		Sophos Email Appliance and XG Firewall	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.
B.4 System security	**Controls against malware** *Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.*	Sophos Intercept X and Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect and remediate threats with ease.
		Sophos Email Appliance	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		XG Firewall	Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access.Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Mobile	Delivers Unified Endpoint Management (UEM) and security management for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
	Network controls *Networks shall be managed and controlled to protect information in systems and applications.*	XG Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
		Sophos Mobile	Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X and Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
B.5 Resilient networks and systems	**Availability of information processing facilities** *Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.*	XG Firewall	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
	Information backup *Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.*	Sophos Email on Central	In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to ensures no email is lost, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is 5 days.

SOPHOS

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
B.6 Staff awareness and training	**Security skills assessment** *Assessment of security skills and addressing skills gaps with appropriate training*	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
Objective C: Detecting cyber security events			
C.1 Security monitoring	**System monitoring and control** *Tracking suspicious user activity and enabling instant incident response*	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X and Sophos Intercept X for Server	Get detailed log events of malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process sensitive data.
		Sophos Intercept X for Server	Prevent unauthorized applications from running with Server Protection that automatically scans your system for known good applications and whitelists only those applications.
		Sophos Firewall/UTM	Get real-time insights into network and user events, quick and easy access to historical data, easy integration with third-party remote management and monitoring tools (RMMs).
		Sophos iView Reporting	Get intelligent centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
C.2 Proactive security event discovery	**Proactively identify events and incidents** *Anomalous events in network and information systems are detected.*	Sophos Synchronized Security	Allows next generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device, allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data to a C2 server; drastically improves incident response time.
		Sophos Intercept X and Sophos Intercept X for Server	Integrated system of prevention, detection, remediation and encryption technologies.

Objective D. Minimizing the impact of cyber security incidents

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
D.1 Response and recovery planning	**Availability of information processing facilities** *Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.*	XG Firewall	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
	Data Recovery Capability *Ensuring reliable data protection and recovery capabilities.*	Synchronized Security	Stops data-stealing attacks at your network perimeter with Synchronized Security that works side-by-side with endpoint protection to automatically identify and isolate compromised systems.
		Sophos Intercept X and Sophos Intercept X for Server	Integrated system of prevention, detection, remediation and encryption technologies.
		SafeGuard Encryption	Proven encryption technology; flexible recovery options for keys, data and forgotten passwords.

The EU Directive on Security of Network and Information Systems (NIS Directive)

SECURITY PRINCIPLE*	GUIDANCE*	SOPHOS SOLUTION	HOW IT HELPS
D.2 Lessons learned	**Build resilient systems** *Continual improvement by assessing events and incidents, and analyzing what has worked and what has not.*	Sophos Intercept X and Sophos Intercept X for Server	Intercept X is continuously looking at reported false positives and false negatives, to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up-to-date over time.

*This content is selected and derived from the Security Principles and Guidance and references published by the UK National Cyber Security Centre at: https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance. Please visit this website for a complete listing of the NIS Security Principles and associated external Guidance and references provided by the UK National Cyber Security Centre. Please consult other EU Member States' websites for information about their implementation of the NIS Directive.

Specifications and descriptions subject to change without notice. Sophos disclaims in full all warranties and guarantees. This document and the information in it do not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2020-04-14 CC-UK [PS]

SOPHOS