Kiteworks

COMPLIANCE BRIEF

Kiteworks and NIS 2 Directive Reduce Cyber Risk

Essential Service and Online Marketplace Organisations: Achieve NIS 2 Compliance and Secure Your Data

The European Union (EU) has proposed the NIS 2 Directive, an EU-wide regulatory framework for managing Information and Communications Technology (ICT) risks and cyber threats in the essential services and online marketplace sectors. Kiteworks reduces complexity through a single platform to protect and manage data exchanges while providing transparent visibility to help businesses demonstrate NIS 2 compliance.

The proposed regulation would require financial entities to ensure the security of their ICT systems and networks and to report major incidents to relevant authorities. It would also establish a coordinated EU-wide approach to cybersecurity and incident response, with national competent authorities responsible for oversight and enforcement. NIS 2 will apply to EU organizations with more than 50 employees and an annual turnover in excess of $10M and any organization that was previously included in the NIS Directive. Kiteworks and a Kiteworks-enabled Private Data Network, deployed on-premises, in the cloud, or hybrid, directly support your ability to be compliant in your sensitive file and email data that you communicate internally and externally. Here's how:

Enforce Compliance With Information System Security Policies

Kiteworks allows customers to standardize security policies across email, file sharing, mobile, MFT, SFTP, and more with the ability to apply granular policy controls to protect data privacy. Admins can define role-based permissions for external users, thereby enforcing NIS 2 compliance consistently across communication channels.

Handle Incidents With Efficiency

Anomaly detection allows for immediate insight into unauthorized access. AI technology detects suspicious events, such as possible exfiltration, and sends an alert via email and audit logs. Through the platform's immutable audit logs, organizations can trust that attacks are detected sooner and maintain the correct chain of evidence to perform forensics. This enables efficient mandatory reporting of any data violations to the Computer Security Incident Response Team (CSIRT) or, if needed, to the European Union Agency for Cybersecurity (ENISA) in a timely manner per the Directive.

Support Business Continuity With Kiteworks' Built-in Disaster Recovery

Maintain accurate records of all activities and technical data with user-friendly tracking displays, allowing audit logs to serve the dual purpose of ensuring that an organization can investigate data breaches and provide evidence of compliance during audits. In the event of a breach, this grants an organization the ability to see exactly what was exfiltrated so that they can get to work immediately on disaster recovery and continue their day to business while maintaining compliance.

Manage Vulnerabilities in Development and Maintenance

Kiteworks enforces a strict secure software development life cycle including extensive security code reviews, regular penetration testing, and a bounty program to keep your data protected. An embedded network firewall and WAF, zero-trust access, and minimized attack surface all work to significantly reduce security risk. Kiteworks also manages one-click updates for customers that have been tested for compatibility of the patch with other system components, allowing timely patches to the operating system, databases, and open-source libraries.

Define and Enforce Basic Cyber Hygiene Practices

ISO has validated Kiteworks to effectively protect your sensitive data from cyber risk (ISO 27001), including when deployed as a cloud service (ISO 27017), and to shield your organization from damaging leaks of personally identifiable information (PII) as validated by ISO 27018. In addition, Kiteworks has a library of compliance certifications, including being SOC 2 compliant and SOC 2 certified. These certifications, along with the single-tenant architecture and multilayered hardening, continue to validate Kiteworks' ability to mitigate data risk with the content management system and keep your basic cyber hygiene practices within NIS 2 compliance.

Protect Data With Encryption

Ensure volume and file level encryption of all data at rest (with AES-256 encryption) and TLS encryption in transit to protect data from unauthorized access, data corruption, and malware. Flexible encryption allows customers to use Kiteworks' end-to-end encryption and bridge to partners with different standards such as OpenPGP, S/MIME, and TLS. Kiteworks' secure email provides encryption and uniform security controls with an email protection gateway, ensuring only authenticated users can read messages.

Establish Access Control Policies and Asset Management

Kiteworks admins set up granular controls to protect sensitive data and enforce compliance policies, enabling business owners to easily manage content, folders, invitations, and access controls to ensure NIS 2 compliance of all content. Access control can be further managed within compliance with geofencing, app data, file type filtering, and email forwarding control.

Verify Users With Multi-factor Authentication

Apply granular MFA and SSO policies by role and location utilizing RADIUS, SAML 2.0, Kerberos, authenticator apps, PIV/CAC, SMS, and more.