RIBBON COMMUNICATIONS
OUR APPROACH TO
INFORMATION SECURITY

Overview

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G and broadband internet. We maintain a keen focus on our commitments to Environmental, Social, and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon, please visit rbbn.com

As a technology company, we deal in information flows and processes. Our customers trust Ribbon to manage their information with the greatest integrity and the strictest controls. We design security features into our products at every stage of the product lifecycle. Similarly, protecting the privacy of customers, employees and all those whose information is entrusted to Ribbon are hallmarks of our responsible business practices.

Our Approach

Ribbon Communications has an Information Security Management System (ISMS) designed to systematically identify, assess, and address security risks. This system adapts to new threats and regulatory requirements to provide protection against cyber threats through established processes and risk assessments that align with ISO 27001:2022 and NIST CSF standards. Certified third-party assessors validate the implementation and certification annually, ensuring the confidentiality, integrity, and availability of information assets. Additionally, BitSight assessment scoring is used to communicate evaluations of the cyber risk landscape to stakeholders. These standards guide the Cyber Security Roadmap presented to senior management and the board annually.

The implementation process includes the establishment of security policies, risk management procedures,

control objectives, and continuous monitoring mechanisms. All employees and relevant stakeholders are engaged through training and awareness programs to foster a culture of security and accountability.
Through ongoing evaluation and improvement, the ISMS supports our strategic objectives, enhances customer trust, and ensures the resilience of our information systems in an evolving threat landscape.
Risk assessments are performed to identify potential vulnerabilities and threats to our information systems. Risks are evaluated based on their likelihood and impact, and appropriate mitigation strategies are implemented accordingly. Access to sensitive information is strictly regulated. Employees, contractors, and third-party users are granted access based on their roles, responsibilities, and the principle of least privilege. Additionally, we employ CCTV and alarm systems to protect vital assets and data storage. Systems and processes are continuously monitored to detect security incidents in real time. Lessons learned from incidents, tabletop exercises and BCP drills are used to refine and improve security measures.

Finally, regular audits and reviews are conducted to maintain governance standards and prevent breaches of that could have negative consequences such as reputational damage, legal action, and loss of stakeholder trust. To address this concern, the above controls implementations safeguard personal data, trade secrets, and other sensitive information from unauthorized disclosure and ensure compliance with relevant legal, regulatory, and contractual requirements, including the Security Exchange Commission (SEC), Sarbanes-Oxley (SOX), General Data Protection Requirements (GDPR), and the California Consumer Privacy Act (CCPA).

The key components of our ISMS include:

1. Information Security Policy: A formal, high-level document that outlines the organization's commitment to information security and sets the direction for the ISMS.
2. Risk Assessment and Treatment: A structured process to identify, evaluate, and prioritize information security risks, followed by the selection and implementation of appropriate controls to mitigate them.
3. Asset Management: Processes to identify, classify, and manage information assets to ensure they are adequately protected throughout their lifecycle.
4. Access Control: Policies and procedures to ensure that only authorized individuals have access to information and systems, based on business and security requirements.
5. Incident Management: A defined approach for detecting, reporting, responding to, and learning from information security incidents to minimize impact and prevent recurrence.
6. Business Continuity and Disaster Recovery: Plans and procedures to ensure the availability of critical information and systems during and after a disruptive event.
7. Compliance and Legal Requirements: Mechanisms to ensure adherence to applicable laws, regulations, contractual obligations, and internal policies related to information security.
8. Human Resource Security: Controls to ensure that employees, contractors, and third parties understand their information security responsibilities before, during, and after employment.
9. Physical and Environmental Security: Measures to protect physical infrastructure and environments that house information systems from unauthorized access, damage, or interference.
10. Supplier and Third-Party Management: Processes to assess and manage risks associated with

external parties that access or process organizational information.

11. Monitoring and Review: Ongoing activities to track the performance of the ISMS, including audits, reviews, and continuous improvement initiatives.
12. Training and Awareness: Programs to educate and raise awareness among staff about information security policies, procedures, and best practices.

Certification: Certain Ribbon operations are certified to the ISO 27001:2022 Information Security Management Quality Standard and undergo annual testing, self-assessments and external audits. Generally, we maintain levels of adherence to this standard with no major non-conformances being identified during such assessments and audits. Participants in the audits include representatives from IT, HR, Legal, Real Estate and Facilities, Customer Support (RibbonCare) and Corporate Quality.

For more insight regarding Ribbon's approach to data protection , please see our Position on Data Protection (Data Privacy).

Supporting Global Sustainable Development

Our Approach to Information Security directly supports UN Sustainable Development Goal (SDG) 9 which calls to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.

- Target 9.1: Develop sustainable resilient and inclusive infrastructures
- Target 9.4: Upgrade industries and infrastructures for sustainability
- Target 9.5: Enhance research and upgrade industrial technologies
- Target 9-C: Universal access to information and communications technology

Governance

The overall executive direction of our information security program is led by Ribbon's Executive Vice President and Chief Operating Officer. The executive direction of our information security program is grounded in a risk-informed, standards-based governance model that emphasizes resilience, agility, and accountability. At its core, the program aligns with NIST CSF and ISO 27001:2022 frameworks to ensure comprehensive protection of data and systems across all environments.

To meet new threats and operational needs, the program is transforming strategically. It focuses on automating control enforcement and monitoring, exploring zero-trust and micro-segmentation, and evaluating robust cloud-native security models for scalable operations. Executive leadership oversees this transformation through engagement, policy alignment, and lifecycle accountability.

This approach ensures that security measures meet compliance requirements while adapting to new challenges effectively.

Disclosure

We report transparently to our stakeholders on information security progress and performance in our annual Sustainability Report, available on our website.

Version 3.3: Nov 2025