

# Unified Cyber Strategy

## Purpose and Scope

Digital information is a foundation to our organization and integral to the success of our business. For the digital health and safety of our members, clients and communities, Haworth Inc. is committed to protecting its information assets and maintaining the confidentiality, integrity, and availability of its data. To achieve this, we have developed a comprehensive Unified Cyber strategy, built on of the NIST 800-53 cybersecurity guidelines and protocols.

This global comprehensive strategic initiative applies to the operations within Haworth Commercial Interiors, including North America and International.

## Foundational Principles

The Haworth Inc. Unified Cyber Strategy is built on three fundamental principles:

- **Standards-Based:** Adheres to industry-recognized standards and best practices, including NIST Cybersecurity Framework, NIST 800-53, and GDPR.
- **Expert-Guided:** Led by certified experts who provide guidance and support throughout the implementation process.
- **Continuous Improvement:** Embraces a cycle of continuous improvement to ensure ongoing effectiveness and alignment with evolving threats and regulatory requirements.

## Monthly Programs and Management Reviews

Haworth's Unified Cyber Strategy defines monthly policy, program and management reviews to ensure ongoing effectiveness:

- **Cyber Architecture & Risk Management Program:** Manages cybersecurity risks and ensures compliance with industry standards.
- **Data Privacy & Governance Program:** Protects sensitive data and ensures compliance with data privacy regulations.
- **Cyber Resilience & Contingency Program:** Develops and maintains a comprehensive disaster recovery plan.
- **Digital Forensics & Incident Response Program:** Investigates and responds to cybersecurity incidents.
- **Observability & Analysis Program:** Monitors and analyzes cybersecurity data to identify threats and vulnerabilities.
- **Personnel Security & Insider Threat Program:** Screens employees and contractors for potential security risks.
- **Acceptable Use & Security Awareness Program:** Educates employees on acceptable use of technology and cybersecurity best practices.
- **Identity & Access Management Program:** Manages user access to systems and data.
- **Endpoint Security Program:** Protects endpoints from malware and other threats.
- **Network & Communication Security Program:** Implements zero-trust principles to secure networks and communications.
- **Secure Supply Chain & Product Development Program:** Ensures the security of the organization's supply chain and products.

## Cyber Risk Management Program

Haworth implements additional Cyber Risk Management policies, software, and processes aligned with ISO 31000-2018 to properly assess and mitigate risk of 1st, 2nd, and 3rd party systems. These processes ensure the following outcomes:

- Identification of essential personnel according to NIST 800-53
- Vendor Due Diligence to understand controls, policies, and agreements to protect data and systems
- System Due Diligence to identify architecture, continuity procedures, and the documentation thereof

- NIST 800-53 Risk Triage to assess areas of focus and need for the system to be compliant, secure, and private
- Full Risk Register to show highest risks in organization by system criticality
- Real time updated Disaster Recovery plan based on the aforementioned data

## Results and Outcomes


The implementation of the Unified Cyber Strategy has resulted in significant improvements in our cybersecurity posture, including:

- Reduced risk of data breaches and cyberattacks
- Improved compliance with industry standards and regulations
- Enhanced employee awareness of cybersecurity best practices
- Increased efficiency and effectiveness of cybersecurity operations
- Improved collaboration and communication between cybersecurity and other business units

In the case of a digital security event, Haworth has a standard incident response planning procedure which is reviewed on an annual basis. First party information security incidents and substantiated complaints concerning breaches of customer privacy or losses of customer data are annually reported through the Corporate Social Responsibility Report.

## Summary

Haworth Inc.'s Cyber Risk Strategy is instrumental in protecting our information assets and maintaining the confidentiality, integrity, and availability of our data. The strategy's comprehensive approach and focus on continuous improvement have enabled us to achieve significant results and outcomes, ensuring the ongoing security of our organization.



**Jerry Winkler**

Global Information Services Vice President