Information Security at Steelcase

April 2024

Introduction

This document is intended to share general information about our cybersecurity and privacy practices with interested customers and other business partners who wish to understand the measures taken to secure Steelcase* systems and data. We do not publicly share specific security details to reduce the risk of this information being leveraged in an attack against the company or its subsidiaries.

To protect Steelcase's information processing systems and data from internal and external security threats, Steelcase adheres to best practices and guidance from the National Institute of Standards and Technology (NIST) - Cyber Security Framework (CSF). Our resulting information security and privacy policies and related practices (collectively, our "**Policies**") are approved by Steelcase executive management and made available to Steelcase personnel. These policies have taken into account, without being certified, applicable industry-standard best practices including, without limitation, the American Institute of Certified Public Accountants (AICPA), Service Organization Control 2 (SOC2), and PCI-DSS. At Steelcase, information security and privacy are an integral part of our daily business processes and are considered critical to meeting the needs of our customers and stakeholders.

These Policies comply with applicable law including the EU General Data Protection Regulation (GDPR). They are regularly reviewed and updated in the event of significant changes to applicable law, Steelcase architecture, or available technologies. Steelcase addresses breaches of its Policies in the case of employees interfering with or otherwise compromising security measures through a formal disciplinary process.

Use of Information and Technology Assets

These Policies address the acceptable use of information, electronic and computing devices, and network resources used to conduct Steelcase business or interact with internal networks and business systems, whether owned or leased by Steelcase, Steelcase personnel, or a third party. Such items are to be used for business purposes in serving the interests of the company, our customers and business partners. All Steelcase personnel, contractors, and other workers at Steelcase and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with our Policies and standards and in compliance with all applicable laws and regulations. Steelcase maintains an inventory of enterprise assets and software.

Data Management

As a global company transacting with customers and other business partners in over 150 countries, Steelcase understands that it must comply with a growing number of data privacy and security requirements. The General Data Protection Regulation (GDPR) is legislation that protects European Union (EU) residents' personal data. The regulation applies whether the EU resident interacts electronically in the EU or globally. Steelcase is committed to the principles of the regulation, leveraging it as a part of our baseline privacy and security practices. Aligned with our commitment to security and privacy of payment card information, Steelcase complies with PCI DSS Level 1 service provider requirements. HIPAA and HITECH impose requirements related to the use and disclosure of protected health information (PHI). Steelcase adheres to HIPAA regulations requiring that covered entities enter into agreements with business associates to ensure that PHI is adequately protected. Steelcase employees are trained in data management, and a dedicated compliance team ensures controls are in place and followed. Steelcase has documented global data retention policies as required by law and to support Steelcase business processes.

Risk Assessment

Risk assessments are performed on information systems, networks, and applications. These assessments identify relevant risks and threats to the organization, estimate the significance of the identified risks and their impact, assess the likelihood of their occurrence, and determine remediation or mitigation actions. Owners of IT Assets are required, per Steelcase policies, to implement these actions.

In addition to strong contracts with vendors and partners, Steelcase has implemented a third-party assessment platform to evaluate the cybersecurity and data protection practices of Steelcase vendors and service providers to ensure they meet all Steelcase requirements, industry standards, and applicable laws and regulations for information security and data privacy.

Access Controls

Steelcase implements robust access controls based on “least privilege” throughout our system architecture. Audit logs of administrator access are maintained and reviewed for compliance purposes. Some IT roles (such as a network admin) may possess multiple accounts, logging in as a standard user for routine tasks, while logging into a privileged account to perform administrative activities. Steelcase requires User IDs and strong authentication (including password requirements and multifactor authentication) to access protected information on Steelcase systems.

Security Controls

Steelcase implements security best practices by leveraging safeguards and security controls based on National Institute of Science and Technology (NIST) as well as the Center for Internet Security (CIS). These controls provide the foundation for mitigating risks to information and information systems. The safeguards are implemented as part of an organization-wide process to manage risk and address diverse requirements derived from mission and business needs, laws, regulations, policies, standards, and guidelines. Controls are reviewed on a recurring basis or as needed for system configuration requirements.

Physical Security

Steelcase’s data centers are equipped with strong physical security controls that comply with industry-accepted security standards. Globally, Steelcase facilities are protected with physical security controls such as electronic controlled access systems, closed circuit (CCTV) security cameras, and security personnel. Activities are monitored by Steelcase Global Security Operations Center 24x7. Access to the Steelcase data centers must follow our data center access policy, which requires all visitors to be escorted. All access to data centers is logged.

Background Checks

Background verification for employment candidates is a mandatory component of Steelcase’s hiring process. All hired personnel acknowledge Steelcase’s confidentiality and non-disclosure policy requirements. In accordance with applicable law, Steelcase’s employee background checks include identity verification and criminal history checks.

Vulnerability Management

Steelcase conducts independent security reviews of its computing environment, including automated vulnerability scans of systems and custom code using commercially available tools and third-party penetration testing partners. Identified vulnerabilities are reviewed, triaged, and remediated. Steelcase applies, tests, and validates software patches and updates before distribution.

Business Continuity and Disaster Recovery

In addition to standard processes and procedures for the backup and recovery of data, Steelcase tests its Business Continuity (BC) and Disaster Recovery (DR) plans twice yearly. These exercises and tests include evacuation drills, tabletop exercises, and functional testing where possible and necessary. The results are documented, evaluated, and scheduled for remediation within the next review cycle.

Security Architecture, Monitoring, and Defense

Steelcase maintains an up-to-date network infrastructure and related architecture diagrams for both on-prem and cloud environments. A robust security architecture that leverages a defense-in-depth strategy protects the network and systems. This protection includes but is not limited to, EDR, XDR, IDPS, behavioral analytics, vulnerability management systems, and SIEMs. Systems are covered by 24x7x365 monitoring, alerting, and remediation. Team members review logs and track, identify, and investigate anomalies routinely and continuously. Steelcase protects log information against tampering and unauthorized access.

Cybersecurity Training and Awareness

Anyone who is provided access to Steelcase IT resources receives, at minimum, monthly cybersecurity awareness training, which covers information security requirements and employee responsibilities. Steelcase personnel responsible for the development and implementation of information security systems are qualified and capable of performing required security-related functions.

Application Security

Steelcase's development lifecycle process includes privacy and security based on design principles when developing applications or integrations. Steelcase’s application security initiatives are based on industry maturity models and include multiple application security tools, code reviews, security vulnerability assessments, and penetration testing.

Incident Response

Steelcase has a formal Incident Response (IR) Plan encompassing information security or privacy incident response procedures.

The IR Plan outlines:

- Roles and responsibilities of the IR Team, available 24x7x365.
- Procedures to respond to a reported incident based on the type of incident and severity.
- Procedures to maintain chain-of-custody for evidence during incident investigations.
- Reporting requirements and mechanisms to support the necessary communications.
- Process for client and third-party notifications (e.g., legal, regulatory, and contractual).
- Root cause analysis and remediation plan following an incident.

Mergers and Acquisitions

Our company may acquire other entities from time to time. Acquisitions include a due diligence period during which we examine the target organization's cybersecurity and privacy capabilities and controls. Post-closing, acquisitions are required to adhere to the same policies and standards as Steelcase Inc.

* In the context of this document, the term “Steelcase” refers to the business entity Steelcase Inc. and all wholly owned subsidiaries and acquisitions globally.