INFORMATION SECURITY

DESCRIPTION

Information is at the core of all business processes performed within Schneider. Most, if not all, business functions at Schneider take in or create information, add to, or enhance information and make decisions using information

Information is an asset that will differentiate Schneider in the transportation marketplace and allow us to achieve a higher competitive advantage. Information Security practices will enable a more efficient and smarter information self-service methodology that is balanced with the right security practices for the protection of Schneider's confidential and intellectual property.

SCOPE OF THE POLICY

All associates, contingent workers, professional services, and temporary workers, and those employed by others to perform work on company premises or granted access to company information or information systems are covered by this policy. Any people not covered by this policy (for example, visitors) must always be supervised by an associate while they are on company premises. Information regarding this policy and its implementation must be made available to all affected personnel by the Schneider manager responsible for the person's performance.

ROLES AND RESPONSIBILITIES

All associates, contingent workers, professional services, as well as those employed by others to perform work on behalf of Schneider are responsible for ensuring that company information assets are used only in proper pursuit of the company's business; information is not improperly disclosed, modified, or endangered; and access to company information resources is not made available to any unauthorized person. The responsibility to protect Schneider's information assets applies to those associates, contingent workers, professional services, and temporary workers while working onsite or accessing any Schneider information or information assets remotely. The responsibility to protect all Schneider information and information assets applies to all Schneider assets regardless of where the asset is located.

The information security management function is responsible for ensuring that appropriate security controls are developed and implemented throughout the company. The information security management function is responsible for the development, implementation, and enforcement of information security policies, and for advising business application and process owners on the adoption of appropriate security policies. Application design and development staff members are responsible for ensuring that security policies and controls are effectively and efficiently implemented within all applications developed or purchased for use by the company. Application design and development staff members are responsible for ensuring the ongoing effectiveness of security policies and controls within the applications.

Infrastructure and operations staff members are responsible for ensuring that security policies and controls are effectively and efficiently implemented within the technical infrastructure and associated operations. Infrastructure and operations staff members are responsible for the ongoing effectiveness of the security policy and controls within the technical environment.

Any associate involved in selecting or purchasing computer systems, associated hardware or application software is responsible for ensuring that this policy can be effectively implemented for that system or application. Any associate involved in selecting or purchasing computer systems, associated hardware, or application software is responsible for ensuring a risk assessment of any new computer systems, associated hardware, or application software is performed and reviewed by appropriate business management prior to using the system or application for business operations. Any associate involved in deploying or implementing computer systems, associated hardware, or application software is responsible for ensuring the system is implemented in accordance with approved configurations and the conditions that were considered during the risk assessment.

INFORMATION SECURITY

Schneider management must evaluate all stored information, applications, and information systems to determine the appropriate controls required to protect the information asset based on the systems' criticality to the business, value to Schneider, and potential value to competitors. In addition, the security management function will conduct ongoing reviews of risks to company information and systems. The Cyber / Information Security Council will oversee the management of risks to Schneider's information and systems.

PRINCIPLES

Schneider has defined the following principles as the foundation of its Information Security Practice:

Information shall be managed as an asset.	Schneider's information shall be managed like any other asset (create, update, secure, dispose) to provide consistent and accurate information in a timely manner to the enterprise. The right information, at the right level of quality, at the right time enables efficient business execution, and a reliable single source of information that is measured.
Data foundational to efficient execution across the enterprise shall be mastered.	Master data management (MDM) is the practice of linking critical data to a single record (the master) to provide a common point of reference throughout Schneider. This enables clear communication and more proficient business functions across the enterprise because everyone knows who or what that information represents. As an example, it is important that all of the following groups are able to identify a particular truck: Linehaul Services/Maintenance, Recruiting/Driver Trainers, Planners/Dispatchers, Drivers and Finance. Being able to reference the same truck in multiple areas ensures: • Multiple drivers are not assigned to the same truck • Planners/Dispatchers are not assigning shipments to a truck that is in for maintenance • Finance is able to tie revenue and cost to the business area responsible for the truck
Information shall be secure.	Relative to "information is an asset", adequate security will be provided to protect our business information from inappropriate access or disruption, while assuring regulatory compliance and managing risk.
Information quality shall be maintained according to its value.	High quality information enables our business to make the proper decisions to meet our company goals. Quality means accurate, timely and comprehendible information with consistent delivery. The ability for end-users to modify data should be restricted to authorized individuals.

POLICY

While all roles at Schneider handle different information, it is each and every Schneider associate's responsibility to:

1. Protect Schneider from harm or risk by handling Schneider's information according to the:

   a. *Information Security Acceptable Use Policy* – This policy outlines the proper use of devices and information used to conduct Schneider business to ensure the protection of Schneider's information assets.

   b. *Information Management Classification Policy* – This policy specifies how Schneider classifies its information assets and the proper ways to handle information within each class.

c. *Information Security Password Policy* – This policy outlines Schneider's expectations for creating and managing passwords to ensure Schneider's information assets remain secure.

d. *Information Security Assets Policy* – This policy ensures the responsibilities for deployment, provisioning, deprovisioning and administration of Schneider technology assets throughout the asset life cycle are clearly assigned and communicated.

e. *Information Security Network Management Policy* – This policy ensures the integrity and security of Schneider's network, communication and collaborations are maintained and managed to support the needs of the enterprise.

f. *Information Security Risk Management Policy* – This policy ensures Schneider information and information systems are properly assessed for risks and risk remediation plans are assigned owners and tracked to completion.

2. Ensure the protection of Schneider associate personal information according to the Schneider Privacy Policies, to include:

a. *Information Security Health Information Protection Policy* – This policy explains the government requirements (HIPAA) for handling group and individual health information to protect it from unauthorized access.

b. *Information Security Personal Identification Information Protection Policy* – This policy describes the personal identification information (PII) that Schneider collects from or about our associates, how it is used and how the company may share that information with other parties.

3. Ensure Schneider keeps information for the appropriate amount of time as defined in the:

a. *Information Management Retention Policy* – This policy explains the importance of keeping and destroying information in accordance with the type of information to support day to day operations and risk management.

b. Information Management Records Retention Schedule – This document specifies the required amount of time each of Schneider's information records are to be retained.

4. Follow and uphold the Information Security principles and related policies.

ENFORCEMENT

Failure to adhere to the principles or related policies, including not exercising reasonable judgment, may be subject to disciplinary action, up to and including termination of employment.

DEFINITIONS

Application Development: The act of programming or writing source code for applications/software.

Agentic AI: a class of artificial intelligence that focuses on autonomous systems capable of making decisions and performing tasks without human intervention. These systems use sophisticated reasoning and iterative planning to solve complex, multi-step problems and interact with various tools and data source.

Associates: Anyone employed either full or part-time by Schneider.

INFORMATION SECURITY

Broadband: Technology that provides high-speed Internet access or access to private networks.

Business Associate: A "Business Associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Cloud Computing: A model for enabling scalable, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Three common service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Content: Refers to any electronic or digital information, such as: documents (e.g. MS Word, Excel, PowerPoint, Visio, PDF, document image, etc.); email (including attachments); texts or instant messages; blogs; web page images and text; and digital assets (e.g. photos, videos, audio, etc.). Content is also referred to as information assets.

Content Generative AI: a type of artificial intelligence that creates original content such as text, images, video, audio, or software code based on user prompts. It uses deep learning algorithms to simulate human learning and decision-making processes, enabling the generation of natural and contextually relevant content.

Contingent Worker: Anyone contracted through a service provider to perform work on behalf of Schneider. Contingent workers are normally managed by a Schneider Associate and perform specific tasks as assigned. Contingent workers may work on-site at a Schneider facility or off-site.

Covered Entities: Are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

Credentials: User name/user id and password used to gain access to information or systems.

Data Authors: Anyone who creates or modifies information. Data authors are responsible for classifying any information they author and ensuring the storage of the information matches its classification.

Data Owners: Schneider designees who have planning and policy-making responsibilities for Schneider's information and data repositories. The Data Owners, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability.

Data Stewards: Schneider designees who are responsible for ensuring all associates in their work group understand how to apply the Information Security policies to their day to day work, follow the information Management policies, properly classify and store their content and adhere to the retention schedule. Additionally, they are responsible for reporting any non-compliance matters to the data owner and the Information Governance Steering Committee.

Dial-up: Technology that uses the public telephone network to establish a connection to the Internet or private network.

Digital Worker account: An account that is used on the backend for integrating specific processes or system services. It is not accessed interactively.

Encryption: Process of encoding information in such a way that eavesdroppers or hackers cannot read it but the authorized parties can.

File Sharing Sites and Services: Services provided via the Internet to store data. Examples of cloud storage services are Box, Drop Box, Amazon Cloud Drive, Apple iCloud, Google Drive, and Microsoft Sky Drive.

Information: Anything spoken, overheard, written, stored electronically, copied, transmitted, or held intellectually concerning Schneider general business, information systems, associates, business partners, or customers, including data and entity types.

Information Asset Owner (IAO): The Information Technology leader directly responsible for the provisioning, deployment or day-to-day management of the information asset.

Information Management: An umbrella term that encompasses all the systems and processes within an organization for the creation and use of corporate information.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Legacy System: An older computer system or application that may not support current standards or requirements.

Minimum Necessary: The standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.

Mobile Devices: Any portable computing device (laptops, smart phones and tablets.)

Operating System: Software that supports a device's basic functions (controls memory, storage, software and hardware). Examples include Windows, UNIX, iOS, Android, and Blackberry.

Password: An arbitrary string of characters that is used to authenticate an account when attempting to log on, in order to prevent unauthorized access to the account.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as name, Social Security Number, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personal Identification Information: Information of an identifiable individual (including Schneider's customers, employees or vendors, including both past and prospective customers, employees and vendors) transferred by Schneider, or its permitted agents, to a vendor under an agreement or under any statement of work, and any information accessed, developed, derived or otherwise created by vendor or vendor personnel in connection therewith.

Privileged Account: An account that can be assigned to a user on any system that has system privileges beyond those of a standard user. Root, local administrator, domain admin and enable passwords are all examples of privileged accounts that have elevated access beyond that of a normal user.

Professional Services: Anyone contracted through a service provider to provide specific services to Schneider. Work is normally directed by the service provider to meet specific service levels and delivery expectations. Professional Services workers may work on-site at a Schneider facility or off-site.

Proprietary Information: Information that is not generally known to the public.

Removable Media: A device that stores data and can be transported from one device to another. Examples of removable media include USB drives, memory cards, CDs, DVDs, digital cameras, smart phones.

INFORMATION SECURITY

Schneider Data: All data and information, including Personal Information: (a) that is submitted to vendor or vendor personnel by or on behalf of Schneider; (b) that is obtained, accessed, developed or produced by vendor or vendor personnel in connection with an agreement; or (c) to which vendor or vendor personnel have access in connection with the provision of services. Schneider Data shall be considered Schneider's Confidential Information.

Sensitive Data: Any data classified as Confidential or Restricted per the Information Classification policy should be treated as Sensitive Data.

Service Account: An account that is used to run a specific process or system service. A Service account is not logged onto interactively.

Shared Process Account: An account that is only utilized for operating kiosks or digital dashboard displays. While it can be logged in interactively, it is restricted by NetBios name within Active Directory and limited to six devices per account.

Standard User Account: A unique user account assigned to a specific individual which provides access to a computer system or network. Also frequently called a *User ID*.

Strong password: A password that is not easy to guess or be discovered in a short period of time including through the use of specialized software.

System Administration: The act of installing, supporting and maintaining servers or other computer systems that are accessed by other people, systems, or services.

Third-Party Computing: Computing services being provided by an external, non-Schneider, provider. The services could be provided on-site at a Schneider facility or offsite at the provider's or other facility.

Test/Training Account: An account used to simulate a person for testing application functionality. This account can be used interactively and adheres to the same standards as a standard user account.

User: Any Schneider associate, contingent worker or professional services provider who has been authorized to access a Schneider information system or application.

Wi-Fi: Wireless technology used to connect devices to the Internet or private networks.

FOR MORE INFORMATION

For more information about the Information Security Policy, contact the Senior Director of Information Security.

Created: 2/1/2015
Last Revised: 05/09/2025
Last Reviewed: 05/09/2025