Data Policy Statement

Purpose

Schaedler Yesco Distribution, Inc. (Schaedler Yesco) is committed to protecting our data and systems as well as the privacy and personal information of both our users and those with whom we do business. This Policy describes how Schaedler Yesco processes and protects data including the personal information of individuals who use our websites, systems and other digital platforms as well as in the context of our offline business activities.

Schaedler Yesco supports the fundamental rights to privacy and data protection as well as compliance with national and international privacy laws. It is applicable to all our employees, officers, and board members, as well as any user of Schaedler Yesco systems for the collection, processing, use, dissemination, transfer and storage of business data and personal information.

Acceptable use

Schaedler Yesco provides access to users of our systems, employee intranet, user website, and mobile applications for specific business-related activities.

- Users who access the Schaedler Yesco systems may use only the computers, accounts, and files for which they have authorization.
- Users may not use another individual's account or attempt to capture or guess other users' passwords.
- Each user is individually responsible for appropriate use of all resources assigned to him/her, including the hardware and software.
- Users must make a reasonable effort to protect passwords and to secure resources against unauthorized use or access.
- Users of Schaedler Yesco systems may not disclose the personal information of any individual without a legitimate business reason (see below for details).
- Users are to be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person(s) is not permitted and could lead to disciplinary action as well as legal action by the recipient of those communications.

Personal information

Why do we collect and use personal information?

Schaedler Yesco collects personal information for various reasons, including:

- To fulfill customer orders and requests;
- To manage customer and prospect relationships;
- Conduct surveys;
- To improve our products, services, and digital content;
- For identity and credential management, including identity verification and authentication;

- To run marketing activities;
- To provide customers with useful and relevant information to their potential business;
- To obtain payment for products and services that have been provided;
- For corporate audit, analysis and reporting;
- To ensure the security of our activities;
- For fraud detection and prevention;
- To comply with all relevant corporate and employment law; and
- To make back-up copies for business continuity and disaster recovery purposes.

What types of information may be collected and stored?

Customers

When a customer contacts Schaedler Yesco we may collect their information such as:

- name, address, telephone number, and email address;
- professional information, such as customer type, job title, purchasing timeframe;
- product and service preferences, contact preferences, marketing preferences;
- and Financial-related information such as bank account details, credit card information.
- When customers browse our website, we may automatically receive their computer's internet protocol (IP) address.

Personal data will only be held for only the period of time for which it is required.

We will not pass customer data to third parties for marketing purposes, without a specific permission from the customer prior to doing so.

Customers may opt out of any future contacts from us at any time.
You can do the following at any time by contacting Schaedler Yesco via the email address or phone number given on the Website:

- See what data we have about you, if any.
- Change/correct any data we have about you.
- Have us delete any data we may have about you.
- Express any concern you have about our use of your data.

Employees

Schaedler Yesco collects personal data required by law upon hire and as needed throughout the course of employment including those details required to ensure legal compliance with all state and federal laws. This information includes, but is not limited to:

- legal name,
- address, phone number,
- Social Security number,
- driver's license number (or other identifying legal documentation); and
- date of birth.

All employees may request information from the Human Resources department regarding what personal data is held on them. Employees may also request alteration of such data at any time if they believe it is incorrect.

Personal data for employees will be retained for the period of time for which it is required by law.

With whom do we share personal information?

In order to provide the best possible service to our customers, prospective customers, and internal users, Schaedler Yesco may share personal data with other entities when necessary.

These third parties may include, but are not limited to, companies contracted for: website hosting; customer relationship management; sales or product support; product development; improvement of services and digital content; data quality checks; security; finance; regulatory, legal, and compliance purposes.

Information may also be shared with our vendor partners in order to provide improved products and services and to collect information in order to resolve service issues, supply delays or quality control concerns.

Employee information may be provided to outsourced services relating to the processing of benefit and health services.

We will not sell or rent any personal information to a third party without express permission from the individual.

Where it is necessary to transfer personal data to relevant third parties, this will be considered carefully before any such transfer takes place.

Cookies

Schaedler Yesco uses “cookies” on our website and mobile app. A cookie is a piece of data stored on a site visitor's hard drive to help us improve your access to our site and identify repeat visitors to our site. For instance, when we use a cookie to identify you, you would not have to log in a password more than once, thereby saving time while on our site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our site. Usage of a cookie is in no way linked to any personally identifiable information on our site.

Security

To protect personal data, Schaedler Yesco will take reasonable precautions and follow best practices to ensure that it is not inappropriately accessed, disclosed, or misused.

- Information that is stored on computers used by Schaedler Yesco personnel should have appropriate password protection and encryption in place.
- Wherever Schaedler Yesco collects sensitive information (such as credit card data), that information is encrypted and transmitted to Schaedler Yesco in a secure way. You can verify this by looking for a lock icon in the address bar and looking for "https" at the beginning of the address of the Web page.
- To access our business system remotely, a VPN is required to protect from intrusion.
- Information stored in cloud services will have limited access and password protection in place.
- Hard copies of personal data will be stored in filing cabinets in secure areas and will be locked.

- Once personal data is no longer required, it will be deleted. This will include both hard and electronic copies of data.
- Servers are secured in a locked room accessible only by authorized personnel.
- All servers are backed up daily with backups stored off site.
- All Schaedler Yesco owned servers and computers are protected by anti-virus software.
- Internal network is protected by a firewall with intrusion prevention rules.

Who is responsible to monitoring for compliance to this policy?

The IT Manager and the Network Administrators will lead the enforcement, monitoring and compliance with this policy. They will work in cooperation with Human Resources and other departments when needed.

Response to Data Breach

Schaedler Yesco will ensure to monitor the use and processing of data and will seek to identify any data breach as soon as is practicably possible.

Upon being notified of a suspected data breach, the Schaedler Yesco will immediately take action to:

1. Confirm whether a breach has occurred.
2. If confirmed, contain the Breach;
    a. Establish whether steps can be taken to recover lost data and limit any damage caused by the breach.
    b. Prevent further unauthorized access to the system.
    c. Reset passwords.
    d. Where applicable, change the access rights to the compromised system and remove external connections.
3. Determine what type of data was accessed and notify the affected individuals if personal information was involved in accordance with applicable state and federal laws.
4. Notify relevant authorities (police), if criminal activity is suspected.

Enforcement

Any Schaedler Yesco personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their business relationship terminated.