



Corporate Headquarters

4341 State Street Road, P.O. Box 220
Skaneateles Falls, NY 13153-0220 USA
Phone: 800.535.6663 Fax: 315.685.3361
www.welchallyn.com



Credit Card Acceptance and Security Policy

All Welch Allyn personnel accepting credit cards for payment of services or goods must protect and secure all credit card data collected, including but not limited to, account information, correspondence, and CVV numbers.

The compromise of any cardholder information should be reported immediately by contacting Mike Besaw via email at michael.besaw@welchallyn.com or by phone at (315) 554-5463 with a complete overview of the incident. Employees can alternatively use the Ethics and Compliance Reporting Hotline 1-800-455-9024 or online at www.mycompliancereport.com (Company ID: WAI).

Data is considered to be secured only if the following criteria are met:

- Only approved processing software programs and hardware with secure communication protocols and/or encrypted connections are used for the processing of electronic transactions.
- Access to credit card and/or electronic payment data and processing should be limited to essential personnel who have been properly trained to handle credit cards or are authorized on a 'need to know' basis.
- Email is **not used** to transmit credit card payment information.
- Fax transmissions, (both sending and receiving) of credit card and electronic payment information is strongly discouraged. If necessary, transmissions are strictly limited to those fax machines whose access is secured and restricted to authorized individuals only.
- All transactions must be processed immediately and documents containing cardholder and card information must be shredded.
 - The card-validation code (CVV) of a credit card is never stored in any form.
 - All credit card numbers will be tokenized when an order is created in SAP.
 - No raw credit card data should be entered into text fields of any order.
 - All credit card and electronic payment data that is no longer deemed necessary or appropriate to store is destroyed or rendered unreadable.
 - The processing and storage of personally identifiable credit card or electronic payment information on Welch Allyn computers and (cloud) servers is prohibited.
 - Credit card or electronic payment information is never downloaded onto any portable devices such as USB flash drives, laptops or notepads.
- No credit card receipt, document, or correspondence of any kind, referencing the transaction shall include more than the last four digits of the account number and/or the month and year of the expiration.
- No Welch Allyn employee, contractor, or agent who obtains access to credit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to a third party other than to Welch Allyn's acquiring bank, depository bank, Visa, MasterCard or American Express), or pursuant to a government request.
- All requests to provide information to any outside party must be reviewed and approved in advance by the Treasurer.

All department leaders and personnel should strictly observe and enforce this policy to ensure that Welch Allyn customer information and privacy is protected to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).