PCI DSS Training

Protecting Cardholder Information

The University of Texas at Dallas
Information Security Office (ISO)
What is PCI DSS?

PCI DSS stands for “Payment Card Industry – Data Security Standard.” Any organization that processes credit or debit card transactions is subject to these security requirements in order to protect cardholder data. The PCI DSS applies whenever UT Dallas stores, processes, or transmits cardholder data, whether a transaction occurs in person, over the phone, or online.

PCI DSS rules apply to credit and debit cards belonging to cardholders such as students, patrons, donors, etc. PCI DSS does not apply to OneCard information stored on UT Dallas systems because UT Dallas is the cardholder.

The full PCI DSS is available here: https://www.pcisecuritystandards.org/
Purpose of Training

A breach of credit card information could cost UT Dallas up to $500,000 in fines, plus over $500,000 in remediation costs.

UT Dallas employees who handle credit or debit card transactions are the first line of defense to protect valuable information attackers will try to compromise.
How can staff take credit cards?

• **In person? Yes.** The Office of Budget and Finance can provide processing terminals to enable credit and debit card transactions in person.

• **Online? Yes.** UT Dallas offers Marketplace as a way to provide goods and services online.

  • **Over the phone? Maybe.** Call centers have special infrastructure to protect data security while taking credit card information over the phone. Contact the Information Security Office for further information.

  • **Forms? No.** UT Dallas staff should never require a patron to enter credit card information on a paper form.
Card Information

A credit card contains several data elements that need to be protected:

- 16 digit Personal Account Number (PAN)
- First and Last Name of Cardholder
- Valid/Expiration Date
- Card Verification Code (CVC)
- Magnetic strip
- EMV Card Chip
Wait, Who are you?

A person presenting a credit or debit card may not be the owner of the card. Confirm the identity of the person by matching a signature, requesting a photo ID, or other verification procedures.

Confirming the identity is required when processing a credit or debit card, looking up information for a refund, or any other time card data is used.

This protects the individual as well as the University.
Protecting Payment Devices

Attackers often attempt to compromise a payment device in order to steal information when a card is swiped. Be alert for changes to the devices you usually use:

- Signs of tampering: check for modifications or add-ons to a device.
- New devices: if upgrades are needed, your management will know about it. If you see something strange, be skeptical!
- Unusual repair technicians: If someone says they are there to fix the device or computer, check with management or the ISO.
- Suspicious behavior: if someone is trying to unplug, open, remove, or replace a device, report the act to management or the ISO.
- Staff are instructed not to install, remove, or repair devices without prior authorization.
Protecting Electronic Records

UT Dallas may process credit or debit card transactions – however, card information (PAN, CVC, PIN numbers, etc.) should NEVER be stored in electronic format.

Card information may NEVER be sent via email, instant messaging, social media, SMS text messages, or similar services.
Protecting Paper Records

Storing card information should be limited – hard copy materials containing card information (e.g., paper receipts, paper reports, faxes, etc.) must be physically secured and accessible only by authorized users, then destroyed securely when no longer needed:

• Hardcopy media must be destroyed by shredding, incineration, or pulping so that cardholder data cannot be reconstructed.

• Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel.

• Be wary of sending materials with card information to others – ask the ISO for guidance if this is necessary.

Better yet, do not save it!
Security Incidents

An incident includes accidental or deliberate exposure of data to unauthorized parties or disruption of security controls.

<table>
<thead>
<tr>
<th>Type of Issue</th>
<th>Who to contact?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security issues</td>
<td>Please email <a href="mailto:infosecurity@utdallas.edu">infosecurity@utdallas.edu</a> or call (979) 883-6810. For anonymous reporting, please use the online form to report an incident: <a href="https://utdallas.edu/infosecurity/report/">https://utdallas.edu/infosecurity/report/</a>.</td>
</tr>
<tr>
<td>Missing / Stolen equipment</td>
<td>Please report missing or stolen credit card terminals to the UT Dallas Police Department at (972) 883-2222. Please contact the ISO after the filing of the police report.</td>
</tr>
<tr>
<td>Noncompliance / Unethical behavior</td>
<td>The Ethics and Compliance Hotline at (888) 228-7702 provides a confidential means to report instances of suspected non-compliance or unethical behavior. This may include financial matters such as fraud, theft of University assets, or conflicts of interest; and other misconduct or violations of UT Dallas / UT System policy.</td>
</tr>
</tbody>
</table>
Congratulations!
You finished the PCI DSS Module

Thank you for taking the time to review this information. This training module will remain available at the [Office of Institutional Equity and Compliance website](https://www.utdallas.edu/eic).