

Credit Card Security Incident Response Policy

Washington University has a thorough information security policy¹. To address credit cardholder security, Visa and Mastercard have jointly established a cardholder information security program (CISP) that provides specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a security incident response team and document an incident response plan. The Washington University security incident response team is comprised of the Supervisor of Cash and Credit Operations, the Associate Vice Chancellor of Computing and Information Systems, and the Director of Computing and Information Systems. The Washington University security incident response plan is as follows:

1. Each department must report an incident to the Supervisor of Cash and Credit Operations.
2. The Supervisor of Cash and Credit Operations will report the incident to the Credit Card Security Incident Response team.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processor, etc) as necessary.
5. The Response Team will determine if policies or processes need to be updated to avoid a similar incident in the future.

References:

1) Washington University Information Security Policy:

<http://www.wustl.edu/policies/infosecurity.html>

2) Visa / Mastercard Cardholder Information Security Program:

http://usa.visa.com/business/accepting_visas/ops_risk_management/cisp.html?it=12//business/accepting_visas/ops_risk_management/cisp%2Ehtml|Cardholder%20Information%20Security%20Program

3) “What To Do if Compromised” link:

<http://visasearch.visa.com/UsaSearch/query.html?col=apac&qt=what+to+do+if+compromised&col=usa&ws=0&st=1>