EMERGENCY RESPONSE POLICY
FOR ANY BREACH OF CREDIT CARD INFORMATION

#1: CONTACT SECURITY OPERATIONS AND SERVICES (SOS)

Employees working in a Credit Card Processing Environment (CPE) must contact ITS Security Operations and Services (SOS) if suspicious activity occurs on a University computer that is processing, transmitting or storing credit card information.

If you experience suspicious activity while processing, transmitting or storing credit card information, you must follow the steps below.

1. If during business hours (Monday through Friday, 8:00 AM to 5:00 PM) make positive contact with SOS immediately by verbally speaking with someone in the office. This should be your first point of contact. Dial 814-863-9533. It is important the computer not be powered off unless directed to do so by SOS.

   If after hours, send an email to security@psu.edu. An SOS staff member will get back to you as soon as possible.

2. Describe to SOS the suspicious activity that is occurring on the computer and indicate the machine is being used for credit card activity.

Examples of suspicious activity (list is not exhaustive):

- Interception of credit card transmission (another program seems to take over or the transmission is routed to an unknown/unfamiliar site)
- Control or access to the computer is taken over by an unknown entity
- Unidentified screens pop-up without command
- Overall operation does not appear the same

#2: CONTACT THE DIVISION OF DEVELOPMENT & ALUMNI RELATIONS INFORMATION SYSTEMS

After you report the suspicious activity to SOS, contact our DDAR Support group at support@ddar.psu.edu.