Security :: Incident Response

California law requires individual notification where the security of personally-identifiable or other confidential information has been compromised.

If you suspect that a computer or system for which you are responsible has been compromised:

- Do not unplug, turn off, disconnect, or otherwise touch the computer in any way UNLESS you strongly suspect that Level 1 [1] protected data is in the process of being removed from the system as a result of the security breach and that your actions would prevent this.
- Contact your supervisor and your ITC [2] immediately.

If the system contains Level 1 or Level 2 [3] data, this is an information security emergency. Telephone the Campus Information Security Office (ISO) at (707) 826-3815 immediately, or ask your supervisor to send an email to security@humboldt.edu [4].

Make no public statements about the incident. All questions must be referred to the ISO during any investigation. After the investigation, specific referral directions will be issued by the ISO.

For after-hours emergencies, please email security@humboldt.edu [4] or call UPD at (707) 826-5555.

Additional information:

IT Staff Procedure to Secure Compromised Systems [5]

HSU Incident Response and Notification Plan (requires HSU login) [6]

Related Topics

Security [7]

Source URL: http://www2.humboldt.edu/its/security-incidentresponse

Links:
[1] http://www2.humboldt.edu/its/glossary/5#term224
[2] http://www2.humboldt.edu/its/glossary/5#term233
[3] http://www2.humboldt.edu/its/glossary/5#term293
[4] mailto:security@humboldt.edu
[5] https://www.humboldt.edu/its/security-compromisedhostprocedure
[6] https://its-sharepoint.humboldt.edu/ITS%20Shared%20Documents/ISO/ITS/HSU-Policies-Procedures-initiatives/HSU%20Incident%20Response%20and%20Notification%20Procedure/HSU%20Incident%20Response%20and%20Notification%20Procedure%20FINAL.pdf
[7] http://www2.humboldt.edu/its/category/quicklinks/security