Appendix B -
System Compromise, Loss, or Theft - Resolution Process

System Compromise, Loss or Theft

SIRT determines where it is and who administers it.

If compromise, SIRT refers incident to appropriate support group for repair. Working with support group, SIRT removes system from network as quickly as possible, images hard drive in case analysis is needed.

CIO contacts appropriate business manager to determine contents of compromised, lost, or stolen system.

Was sensitive info on the machine?

Yes

Convene Ad Hoc group to research the compromise and develop recommendations for action, if appropriate.

No

Repair complete. With business manager approval, SIRT moves system back to production network.

incident Closed

Does incident require action?

Yes

Incident referred to President and Vice-Presidents. PR is engaged if communications are necessary.

No

incident Closed

incident Closed

Appropriate Action Taken. Incident Closed.

January, 2008