6. Respond to Intrusion

6.1 Identify the incident
6.2 Notify CERT team.
6.3 Containment.
6.4 Eradicate
6.5 Restore system
6.6 Harden network security
6.7 Follow Up

6.5.1 Restore system from a safe, uncompromised backup
6.5.2 Harden System
6.5.3 Notify users of restored system.

6.3.1 Isolate the compromised system.
6.3.2 Backup compromised systems.
6.3.3 Examine logs on system, firewall, routers, and other network monitors.