**Incident Response Procedures**

1. **Alert/Notification/Detection of Incident**
   - Submit a ticket to the ITSS helpdesk or verify ticket has been submitted
   - Major Incident?
     - Yes
       - Forensic Image
       - Eradication of the Incident
         - Create image of system for forensic investigation
         - Determine and if appropriate remove the cause of the incident
         - Restoration of the System
           - Restore system from backup if necessary
           - Apply appropriate patches
           - Verify system is back to normal operation
           - Place system back on-line and monitor
         - Follow-Up
           - Notify UND ITSO of resolution
           - ITSO will document lessons learned and publish best practices
         - END
     - No
       - Private or confidential data involved?
         - Yes
           - ITSO/CIO will decide if it is necessary to convene the Information Security Incident Response Team (ISIRT)
         - No
           - Containment of the Incident
             - Disable network access
             - Change password
             - End
   - No
     - Incident Reporting
       - Notify UND ITSO (directly 777-3587, email itsecurityofficer@und.edu, helpdesk 777-2222)
       - Notify Data Steward and/or Unit Head/Dean
       - ITSO/CIO will decide if it is necessary to convene the Information Security Incident Response Team (ISIRT)

---

**Major Incident Identification**
- Involves a device with private or confidential data
- Threatens business continuity
- Affects multiple systems or servers
- Has the potential to threaten UND’s reputation

---

**Revised 12/06/06**