1. **Type of Incident** (Check all that apply)
   - □ Computer System
   - □ Inmate Action
   - □ Physical (Loss/Theft)
   - □ Intentional Breach
   - □ Unintentional Act
   - □ Other: ____________________

Staff Involved:

<table>
<thead>
<tr>
<th>Name:</th>
<th>Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number:</td>
<td></td>
</tr>
<tr>
<td>Computer Workstation Name (if applicable):</td>
<td></td>
</tr>
</tbody>
</table>

Inmate Involved:

<table>
<thead>
<tr>
<th>Name:</th>
<th>SID:</th>
</tr>
</thead>
</table>

Scope of incident:  
   - □ Network/System
   - □ Single User Account
   - □ Isolated Incident
   - □ Credit Card Information

How long since this incident happened: ____________________

How critical do you think this incident is, and why? ____________________

1. **Protect/Contain:**
   - **Computers:** Stop use of involved/affected computer equipment.
   - **Physical Security:** Restrict access to affected areas as appropriate.
   - **Inmates:** Review need for Administrative Segregation placement. Secure cell (and work area if appropriate) pending investigation.
   - **Communication:** Direct staff to not discuss the incident with anyone but you until further notice.

2. **Notifications/Reports:**
   - Notify the Information Security Officer (ISO) as soon as possible for assistance in determining level of response. If the breach contained credit card information, identify the specifics to the ISO.
   - Notify Special Investigations Unit (SIU) for incidents involving inmates.
   - After Hours: ODOC Help Desk should be notified immediately of any incident involving computers or related network.
   - Unusual Incident Report will be required for all Information Security incidents.

Additional resources:
- DOC Policy 60.1.6 Information Security Incident Response
- ODOC Information Security Incident Response Plan

Contact Information:
- Dave Wilson, ISO: 503-991-0926
- Help Desk: 1-866-531-9600

CD 1580 (2/12)