

# Oregon Department of Corrections

## Information Security Incident Supervisors Checklist

---

---

**1. Type of Incident (Check all that apply)**

- Computer System     Inmate Action     Physical (Loss/Theft)  
 Intentional Breach     Unintentional Act     Other: \_\_\_\_\_

**Staff Involved:**

Name:	Location:
Phone number:	
Computer Workstation Name (if applicable):	

**Inmate Involved:**

Name:	SID:
-------	------

**Scope of incident:**     Network/System     Single User Account     Isolated Incident

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 till further notice.

**2. Notifications/Reports:**

- Notify the Information Security Officer (ISO) as soon as possible for assistance in determining level of response.
- 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