Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Best Practices for the Prevention and Detection of Cyber Insider Threat

- Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.
- Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.
- Consider insider threats in the software development life cycle.
- Use extra caution with system administrators and technical or privileged users.
- Implement system change controls.
- Log, monitor and audit employee online actions.
- Anticipate and manage negative workplace issues.
- Track and secure the physical environment.
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege.
- Use layered defense against remote attacks.
- Deactivate computer access following termination.
- Implement secure backup and recovery processes.
- Develop an insider incident response plan.
- Report suspicious or illicit IT insider activity through appropriate channels.