Activity 2.2.4 - SANS Clean Desk Policy Study Guide

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribue a new policy or updated version of this policy, please send email to* policy-resources@sans.org

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. **Overview:** A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. **Purpose:** The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" - where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in a locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 complaint, but it is also part of standard basic privacy controls.

3. **Scope:** This policy applies to all <Company Name> employees and affiliates

4. **Policy:**

   4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

   4.2 Computer workstations must be locked when workspace is unoccupied

   4.3 Computer workstations must be shut completely down at the end of the work day.

   4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

   4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

   4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

   4.7 Laptops must be either locked with a locking cable or locked away in a drawer.

   4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

   4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

4.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

4.12 Lock away portable computing devices such as laptops and tablets.

4.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your ogranization.*

5. Policy Compliance:

5.1 Compliance Measurement - The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions - Any exception to the plicy must be approved by the Infosec team in advance.

5.3 Non-Compliance - An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes:

7. Definitions and Terms