Clear Desk and Clear Screen Policy Template

Document Control Information

- **Document Title:** Clear Desk and Clear Screen Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Clear Desk and Clear Screen Policy establishes [ORGANIZATION NAME]'s requirements for maintaining a clean and secure work environment in accordance with ISO 27001:2022 requirements. It provides guidelines to reduce the risk of unauthorized access, loss, or damage to information during and outside normal working hours.

1.2 Scope

This policy applies to: - All employees, contractors, consultants, temporary staff, and other workers - All work areas, including offices, cubicles, shared spaces, and remote work locations - All information in physical and electronic form - All computer equipment, mobile devices, and storage media - All hours of operation, with special emphasis on periods when workspaces are unattended

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Protecting sensitive and confidential information from unauthorized access - Reducing the risk of information theft, fraud, or compromise - Maintaining a professional and organized work environment - Complying with data protection and privacy regulations - Promoting good security practices among all personnel

2. Clear Desk Requirements

2.1 During Working Hours

- Sensitive documents must be removed from desks when not in use
- Documents requiring disposal must be shredded or placed in designated secure disposal bins
- Storage media (USB drives, external hard drives, etc.) must be secured when not in use
- Access cards, keys, and other physical access devices must be secured
- Passwords must not be written down and left in accessible locations
- Whiteboards and flipcharts containing sensitive information must be erased after use

2.2 Short Absences

When leaving a desk for a short period: - Computers must be locked (e.g., using Windows+L or equivalent) - Sensitive documents must be removed from plain view - Mobile devices must be secured or taken with the user - Meeting rooms must be cleared of notes and documents

2.3 End of Day

At the end of the working day: - Desks must be cleared of all documents and papers - All sensitive materials must be locked in drawers or cabinets - Computers must be shut down or hibernated according to IT requirements - Cabinets and drawers containing sensitive information must be locked - Keys to cabinets must be secured and not left in locks - Printers and fax machines must be cleared of documents - Waste bins must be emptied into secure disposal containers if they contain sensitive information

2.4 Remote and Home Working

When working remotely or from home: - The same clear desk principles apply to home workspaces - Sensitive information must be stored securely when not in use - Family members and visitors must not have access to work-related information - Documents must not be left in vehicles or public places - Secure disposal methods must be used for sensitive information

3. Clear Screen Requirements

3.1 During Working Hours

- Computer screens must be positioned to prevent unauthorized viewing
- Privacy screens should be used in high-traffic areas or open office environments
- Sensitive information must not be displayed when others are present
- Projectors and shared displays must be turned off when not in use
- Meeting room displays must be cleared after presentations

3.2 When Unattended

When leaving a computer unattended: - Screens must be locked using a password-protected screensaver or equivalent - Applications containing sensitive information must be closed - Remote desktop connections must be terminated - Mobile device screens must be locked

3.3 Automatic Controls

The following automatic controls shall be implemented: - Password-protected screen savers must activate after [10-15] minutes of inactivity - System sessions must time out after [15-30] minutes of inactivity - Authentication must be required to unlock screens or resume sessions - Mobile devices must automatically lock after [1-5] minutes of inactivity

4. Information Handling

4.1 Document Classification

- Documents must be classified according to the Information Classification Policy
- Handling requirements must be based on classification level
- Highly sensitive documents require additional security measures

4.2 Document Storage

- Adequate secure storage must be provided for sensitive documents
- Filing cabinets, drawers, and safes must be locked when not in use
- Storage areas must be secured against unauthorized access
- Electronic documents must be stored in appropriate secure locations

4.3 Document Disposal

- Paper documents must be disposed of using approved methods:
  - Non-sensitive: Regular recycling
  - Sensitive: Cross-cut shredding or secure disposal bins
  - Highly sensitive: Secure destruction with verification
- Electronic media must be securely wiped or physically destroyed
- Disposal must comply with data retention requirements

5. Physical Security

5.1 Office Access

- Office areas must be secured against unauthorized access
- Visitors must be escorted in areas where sensitive information is processed
- Staff must challenge unescorted visitors or unknown individuals
- After-hours access must be restricted and logged

5.2 Workspace Design

- Open plan offices should incorporate privacy measures
- Screens should face away from public areas, corridors, and windows
- Printer and fax areas should be monitored or restricted
- Lockable storage should be provided for all staff

6. Roles and Responsibilities

6.1 All Personnel

- Comply with all aspects of this policy
- Secure sensitive information when not in use
- Lock screens when leaving workstations unattended
- Report security incidents or policy violations

6.2 Managers

- Ensure staff are aware of and comply with this policy
- Provide adequate secure storage for their teams
- Conduct periodic checks for policy compliance
- Address non-compliance through appropriate channels

6.3 Security Team

- Monitor compliance with this policy
- Provide guidance on secure storage and disposal
- Investigate security incidents related to clear desk/screen violations
- Recommend improvements to physical security measures

6.4 IT Department

- Implement technical controls for screen locking
- Configure automatic timeout settings
- Provide secure disposal methods for electronic media
- Support secure remote working capabilities

7. Compliance and Monitoring

7.1 Regular Inspections

- Random spot checks will be conducted to verify compliance
- After-hours inspections may be conducted with appropriate authorization
- Compliance will be included in security audits
- Results will be reported to management

7.2 Non-Compliance

- Instances of non-compliance will be documented
- Repeated violations will be escalated to management
- Disciplinary action may be taken for serious or repeated violations
- Security awareness training will be provided to address knowledge gaps

7.3 Exceptions

Exceptions to this policy shall be: - Documented with justification - Approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

8. Training and Awareness

- All personnel shall receive training on this policy during onboarding
- Regular reminders shall be included in security awareness programs
- Visual aids and reminders shall be posted in work areas
- Policy updates shall be communicated promptly to all staff

9. Related Documents

- Information Security Policy
- Information Classification Policy
- Physical Security Policy
- Data Protection Policy
- Remote Working Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

10. Approval

This Clear Desk and Clear Screen Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________