Clear Desk and Screen Policy

Version:	1.5	Status:	Approved
Author/Owner:	Digital Services Manager	Approval/Review:	KITGG
Approval Date:	18 March 2019	Next Review Date:	31 March 2020

Introduction

1. This policy details the necessary controls to reduce the risk of an information security breach caused by information being left unattended or being read from an unattended screen.

Scope

2. This policy is mandatory for all employees, contractors and consultants employed by Audit Scotland. Failure to comply with this policy may result in disciplinary action.

3. This policy applies to all areas where Audit Scotland work occurs including client sites, travel and working from home.

Information Classification

4. Audit Scotland uses three information classifications:

   4.1. Public – Information which has been published or would be readily released under a Freedom of Information (FOI) request.

   4.2. Controlled – Information that has not been published and would require review before sharing with others.

   4.3. Personal – Information as defined under Data Protection legislation and would not be released unless it is lawful to do so.

Clear Desk

5. During the day when desks/rooms/offices are unoccupied for an extended period, all information regardless of classification must be cleared from the desk and securely stored.

6. Personal information must be cleared and securely stored whenever a desk is unoccupied.

7. Out with office hours no information shall be left on desks.

8. All personal / controlled documents no longer required must be disposed of in a secure manner in the locked confidential waste containers located around the office.
9. Devices must be kept secure outside of normal working hours.
10. No personal or controlled information shall be left in meeting rooms, either on the table, slides, flip charts, TV screens or whiteboards.

Clear Screen

11. When leaving a desk for **any period**, staff must ensure that devices are locked, to prevent unauthorised access to information or systems.
12. Outside working hours, all unattended devices must be powered off, unless granted specific approval by a member of the Digital Services Team.
13. Device screen timeouts must be set to an appropriate period and password protected.
14. Where possible screens should be angled away from public areas, to prevent unauthorised viewing.

Clear Printers

15. Staff must not leave a printer unattended when printing or scanning:
    - 15.1. Personal information found unattended at a printer must be passed to Corporate Governance for disposal.
    - 15.2. Unattended documents located at a printer or scanner must be securely disposed of.

Staff Awareness

16. Personal information must not be visible to unauthorised personnel.
17. All staff should familiarise themselves with guidance on clear desk and clear screen policies.

Change Log

Version	Date	Author	Description
1.0	02/03/16	IT Manager	Policy created as per ISO certification preparation. For
1.0	03/03/16	ISMT	Approved by ISMT
1.1	10/03/16	IT Manager	Additional ISO requirements added. For KITGG approval.
1.2	11/03/16	IT Manager	Minor amendments made by KITGG and policy approved.
1.3	01/03/17	IT Manager	Scope updated to include client sites and working from home and step added to report personal information found. Minor amendments made and policy approved by KITGG.
1.4	22/03/18	Digital Services Manager	Annual effectiveness review and approved by KITGG.
1.5	18/03/19	Digital Services Manager	Annual effectiveness review by KITGG. Minor updates were made and the policy approved.