POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE User Clear Screen and Desk Policy**
Effective Date:	**14 Feb 2019**
Reference Number:	**ISMS-03-02**
Version Number:	**1.9**
Owner:	**Information Security Manager,**
Review Date:	**03 Jul 2021**

Table of Contents

1. Purpose

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted and users should ensure that unattended equipment has appropriate protection. In particular, the privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation.

This document details the clear screen and desk policy to protect information made available via the TRE from unauthorised and unintended access and distribution.

2. Scope

The scope of this policy is TRE staff and users, their PCs, laptops, other electronic and hardcopy media and any desk and workspace where they are situated.

Electronic media includes but is not limited to:
- Smart phones
- Tablets
- Hard drives
- USB sticks
- CD/DVD

Hardcopy media includes but is not limited to:
- Paperwork
- Letters
- Printouts
- Post-its
- Notebooks/address books
- Whiteboards

3. Responsibilities

TRE Staff and users are responsible for:
- Applying the clear screen and clear desk policies to their workspace.

4. Procedure

4.1. Clear Screen Policy

In order to prevent unauthorized access to electronic information all TRE staff and users shall:
- Lock their PC, laptop or tablet if they intend to leave it switched on and unattended in the office at any time. Note: Users must not rely on the screen-saver to lock the system after a period of idle time.
- Switch off or lock PC's, laptops and tablets before leaving the office.
- Laptops should always be secured with an appropriate lock (e.g. Kensington desk lock) or locked in storage areas when not in use.
- Be aware that screens can be viewed through office windows.

4.2. Clear Desk Policy

In order to prevent unintentional sharing of information all TRE staff and users shall:
- At the end of the working day or when leaving the office for more than 30 mins, clear their desk of hardcopy media containing personal or sensitive information.
- Store hardcopy media in lockable storage cupboards.
- When necessary, dispose of hardcopy media in accordance with SOP-07-03: Disposal of documents**.**
- Store removable electronic media in lockable storage areas when not in use.
- Clear all meeting rooms and breakout areas of all papers and any electronic equipment. Whiteboards should also be cleared of personal or confidential information.
- Use the shredder and bins provided for the disposal of all sensitive and confidential paper waste. The disposal of business sensitive or personal information in non-secure waste will be considered an information security event.
- Use electronic versions of documents and avoid the use of printed material if possible.

In general, exercise due caution with all personal, confidential and business sensitive information. Adhere to the Information Security Policies as information protection is your responsibility.

If in doubt about the confidentiality of the information in your possession treat it as highly restricted and handle it accordingly. See ISMS-07-04: Information Classification for definitions.

5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-07-04	ISMS\Policy & Guidance\Information Governance - policy & guidance	Information Security Classification
SOP-07-03	ISMS\SOP\Information Governance - SOP	Disposal of Sensitive Documents

6. Appendices

None