1. DEFINITION

Information Security Standard **N-SI-002** complements the overall Information Security Policy by defining the Clean Desktop and Screen Policy establishes guidelines and procedures to reduce the risk of security breaches, fraud, and information theft.

2.1. PURPOSE

A Clean desktop and screen policy consists of information security practices recommended in the workplace to avoid unnecessary exposure of information considered sensitive, whether it is personal or business data.

To reduce the risk of unauthorized access, loss or damage to information during working hours and beyond, the BBC has decided to adopt a 'clean desktop' policy for paper and portable media, and a 'clean screen' policy for computers and the like.

No confidential information may be left, whether on paper or on any devices, electronic or otherwise. Information left on the work desktops are liable to be damaged, destroyed or stolen.

The main goal of the Clean Desktop and Screen Policy is to prevent security breaches, fraud and information theft, all through cultural change.

3. WHAT IS INFORMATION?

Information is the result of data processing that adds knowledge to the person receiving it.

Information is a core business asset of an organization and must be adequately protected regardless of the type of media it resides on or wherever it resides.

3.1. PRACTICE SAFE STORAGE

Critical business information should be stored in a secure location when not in use, especially when there are no people in the work environment.

3.2. PCS, MOBILE DEVICES, ETC.

Keep them turned off or protected by password-controlled screen operation or similar authentication mechanisms when visually unattended or not in use.

3.3. TAKING CARE OF PRINTING AND FAXING

Documents with sensitive information: collect them immediately to prevent unauthorized access to the information. If you are using a confidential document, try to keep it in a folder or turn the page, keeping the information and leaving the "blank" side visible.

Incoming and outgoing mail points: protect them and monitor them.

Photocopiers and other reproduction technologies (scanners, digital cameras, etc.): Avoid unauthorized use and use password printing.

3.4. AVOIDING UNNECESSARY PRINTING

The policy also aims to help reduce the amount of paper, thereby reducing unnecessary printing and costs.

Don't print documents just to read them. In other words, read them on the screen if possible.

3.5. CARE OF TRASH

All waste that contains proprietary or secret information must be destroyed using a shredder or shredder or similar machine, or even by manual destruction.

Always make sure that the disposal is done in the right way and that it makes any recovery attempt impossible.

4. INFORMATION SECURITY - CLEAN DESKTOP

"Clean desktop" refers to guidelines that reduce the risk of security breaches, fraud, and information theft, typically caused by documents that are left in plain view on company premises and typically exposed outside normal business hours.

5. PRINCIPLES TO TAKE INTO ACCOUNT

- Paper documents and electronic media should not be left unnecessarily on the desk and should be stored in locked cabinets or drawers when not in use, especially out of office hours;
- Sensitive or business-critical information of the organization, especially sensitive personal data, should be **locked** away in a separate, secure location;
- Notes, memos, and reminders should not be left displayed on the desk or taped to walls, partitions, or the computer monitor;
- Do not write down sensitive information on whiteboards;
- Do not store folders with sensitive documents on easily accessible shelves;
- Destroy the printed documents before throwing them away;
- Don't print documents just to read them. Read them on the screen of your most frequently used device (Paperless Culture);
- Sensitive or confidential information, when printed in a collective location, must be removed from the printer immediately;
- Photocopiers must be protected from unauthorized use;
- Return as soon as possible all documents obtained through loans from other departments when they are no longer needed;
- Computers and printers should not be left "logged in" if the responsible user is not present;
- Storing diaries and notebooks in a locked drawer;
- Store your personal belongings in drawers or cabinets, and if they contain sensitive personal data, they should be locked;
- Never write down passwords on reminders at work;
- Do not leave media, such as CDs or floppy disks, in the drives;
- If possible, position desks and furniture so that confidential data is not visible from windows or hallways;

- At the end of the working day or in the event of prolonged absence from the workplace, clean your desk, put documents in drawers and/or cabinets if they contain sensitive personal data and lock them with a key; switch off computers and equipment;
- Keep drawers and cupboards closed, and those containing sensitive personal data should be kept locked, and it is important not to leave keys in the lock;
- Do not place or eat meals and snacks on the table;
- Do not place glasses of water, juice, soft drinks or coffee on the table;
- Always clean your workstation before you leave it, making sure workpieces are stacked correctly.

6. BASIC RULES OF CONDUCT (IN AND OUTSIDE THE ORGANISATION).

A set of behaviors to be observed inside and outside the organization, with an emphasis on protecting corporate information.

It is essential for the professional to be restrained when representing the company, to be careful in their opinions, conversations, participation in events, when communicating with clients or third parties.

7. FINAL REMARKS

- The guidelines and procedures described in this document can and should be amended as necessary, in which case the amendments/developments should be communicated to the entire organization;
- This policy applies to all employees of BBC INDUSTRIA E COMERCIO LTDA;
- People engagement is vital to the implementation of the Clean Table and Screen Policy.