|  |
| --- |
| building Sam Bailey19/11/2025 Clean Desk Policy Report |
|  |

## Introduction

This report looks at the CITEMS Clean Desk Policy and checks how well it covers the physical security risks mentioned in the article “Police Warning: Cyber Criminals Are Using Cleaners to Hack Your Business.” The main goal is to see where the policy lines up with modern threats, where it falls short, and what extra steps could be taken to improve physical information security.

## Recent Policy Changes

The Clean Desk Policy was recently introduced to improve workspace hygiene and reduce the risk of data being exposed. Some of the main points include:

* Keeping desks clear when they’re not being used
* Storing documents and devices safely
* Making sure computers are locked when unattended
* Disposing of sensitive materials securely
* Removing confidential notes from whiteboards

## Summary of Article Findings

The article explains that cyber-criminals are now taking advantage of physical access, especially through cleaning and maintenance staff. It mentions that organized crime is deliberately using after-hours cleaners to get into workplaces, where they might photograph documents, plug in malicious USB devices, or take data left out on desks or in meeting rooms. The article also points out that even businesses with strong digital security can still be at risk if their physical spaces aren’t protected. It finishes by stressing that good workplace habits, strong awareness, and clear rules around workspace security are needed to deal with these threats.

## Alignment Between the Policy and Identified Threats

**In line with the article:**

* The policy requires desks to be clear of sensitive material, which lowers the chance of people seeing information that shouldn’t be left out.
* Storing documents and devices in locked areas helps protect them further.
* Mandatory computer locking matches the article’s warning that unlocked screens are an easy way for criminals to get into a system.
* Clearing whiteboards after meetings also fits the article’s point that meeting notes are often left visible and can be photographed.
* Secure disposal methods, like shredding, help stop sensitive information from being taken out of regular rubbish.

**Not in line or missing:**

* The article talks about the risk of cleaning contractors being used as insider threats, but our policy doesn’t mention interacting with contractors in the workplace would work.
* We don’t mention monitoring after-hours access into the building or office areas.
* The article also highlights the danger of malicious USB devices, but the Clean Desk Policy doesn’t address removable media being left out.
* Our policy mainly focuses on individual workspaces and doesn’t clearly cover meeting rooms, printers, or shared areas, which the article identifies as risks.

## Conclusion

Overall, the Clean Desk Policy covers most of the basic protections mentioned in the article, like keeping sensitive info out of sight and securing devices. But the article also points out newer risks, especially around third-party cleaners, that the policy doesn’t really cover. Adding a few controls in that area would help close those gaps.

## Recommendations

To better match the threats highlighted in the article, the policy could include:

* Staff training on spotting suspicious behaviour from contractors or people who shouldn’t be in the area.
* Guidance on USB and other removable media risks, including making sure no devices are left out.
* An update to cover shared areas like meeting rooms, printer stations, and break rooms.

## Email

