Synthetic Users Clean Desk / Clear Screen Policy

Version: 1.0

Effective Date: 25 March 2026

Last Reviewed: 25 March 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy establishes requirements for maintaining clean desks and clear screens across all Synthetic Users work environments — including remote workstations and the Lisbon studio — to protect sensitive information, including JPMC confidential data, from unauthorized access, loss, or disclosure.

2. Scope

This policy applies to all Synthetic Users employees, contractors, and temporary staff who access company systems or handle sensitive information, whether working remotely or from the Lisbon studio.

3. Clean Desk Requirements

3.1 General Principles

- Sensitive or confidential documents (printed or handwritten) must not be left unattended on desks, tables, or shared surfaces.
- At the end of each workday, or when leaving a workstation unattended for an extended period, employees must clear their workspace of all sensitive materials.
- Sensitive documents that are no longer needed must be disposed of securely (e.g., shredding or secure disposal bins).

3.2 Physical Storage

- When not in active use, sensitive documents must be stored in locked drawers or cabinets.
- Portable storage media (USB drives, external hard drives) must be secured in locked storage when not in use.
- Whiteboards and shared display surfaces must be erased of sensitive content after meetings.

3.3 Remote Work Considerations

- Remote employees must ensure their home workspace is free of sensitive materials when not actively working.
- Printed confidential documents should be minimized; digital workflows are preferred.
- If printing is necessary, documents must be collected immediately and securely disposed of when no longer needed.

4. Clear Screen Requirements

4.1 Automatic Screen Lock

- All company-issued MacBooks are configured to automatically lock after a maximum of **5 minutes of inactivity**, as enforced by the Endpoint Security Policy.
- Screen lock timeout is monitored and enforced through **Sprinto (Dr. Sprinto MDM)**.

4.2 Manual Screen Lock

- Employees must manually lock their screens (Cmd+Ctrl+Q on macOS) every time they step away from their workstation, even briefly.
- This applies in all environments: home offices, the Lisbon studio, co-working spaces, and public locations.

4.3 Screen Privacy

- Employees working in public or shared spaces must position their screens to minimize the risk of shoulder surfing.
- Privacy screen filters are available upon request for employees who frequently work in public-facing environments.

5. Studio-Specific Controls (Lisbon Office)

- Meeting room whiteboards and displays must be cleared of sensitive information after each session.
- Shared desks (hot-desking areas) must be fully cleared at the end of each use.
- Visitors must be escorted and must not be left unattended in areas where sensitive information is accessible.
- Printers in shared areas require secure print release (pull printing) to prevent uncollected printouts.

6. Enforcement & Compliance

6.1 Monitoring

- Periodic spot checks of the Lisbon studio are conducted by the Security & Compliance Lead to verify compliance.
- Endpoint compliance (screen lock configuration) is continuously monitored via Sprinto.
- Non-compliance findings are documented and tracked to resolution.

6.2 Employee Awareness

- Clean desk and clear screen practices are included in the annual Security Awareness Training program (see User Awareness Training).
- New employees receive clean desk/clear screen guidance as part of onboarding.

6.3 Violations

- First-time violations result in a documented reminder and re-training.
- Repeated violations are escalated to the employee's manager and may result in disciplinary action in accordance with the Employee Code of Conduct.

7. Related Documents

- Endpoint Security & Device Management Policy
- Remote Access Policy
- User Awareness Training Program
- Employee Code of Conduct
- Acceptable Use Policy

8. Review Schedule

This policy is reviewed annually or upon material changes to the work environment, security architecture, or client requirements. Next scheduled review: **March 2027**.