[Company]

CLEAR DESK AND CLEAR SCREEN POLICY

Maintaining a clear desk and clear screen of confidential information

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

1 Document Version Control 2

2 Document Contents Page 3

3 Clear Desk and Clear Screen Policy 5

- 3.1 Purpose 5
- 3.2 Scope 5
- 3.3 Principle 5
- 3.4 Internal, Confidential and Critical Information 6
- 3.5 Printers, Photocopiers and Reproduction Technology 6
- 3.6 Cash, Cheques, Bank Cards, Payment Devices 6
- 3.7 Media Disposal 7
- 3.8 Desk Cleaning 7
- 3.9 Pop-ups and Notifications 7

4 Policy Compliance 8

- 4.1 Compliance Measurement 8
- 4.2 Exceptions 8

4.3 Non-Compliance 8

4.4 Continual Improvement 8

5 Areas of the ISO27001 Standard Addressed 9

3 Clear Desk and Clear Screen Policy

3.1 Purpose

The purpose of this policy is to reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours.

3.2 Scope

All employees and third-party users.

Confidential information in electronic and paper form.

Monetary items and associated resources.

3.3 Principle

Clear desk and clear screen are ensuring that resources of value and confidential information are secured from unauthorised access, loss, or damage when not in use.

3.4 Internal, Confidential and Critical Information

Internal, confidential, or critical business information, e.g., on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or desk or other forms of security furniture) when not required, especially when the office is vacated.

Computers and terminals should be [redacted]

Whiteboards and other types of display are cleared or cleaned of confidential or critical information when no longer required.

3.5 Printers, Photocopiers and Reproduction Technology

Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented.

Media containing confidential, internal or is deemed in other ways sensitive information [redacted]

3.6 Cash, Cheques, Bank Cards, Payment Devices

All items that are payments or able to take or make payments are to be physically locked away securely when not in use.

3.7 Media Disposal

Media should be destroyed in line with the [redacted] [redacted] but as summary internal and confidential should be placed in the confidential waste bins or company provide shredders where available and never in general waste.

3.8 Desk Cleaning

All desks and other workspaces should be sufficiently tidy at the end of each working day to permit the cleaning staff to perform their duties.

3.9 Pop-ups and Notifications

Screen pop-ups and notifications, such as messaging and new email alerts, should be [redacted]

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.