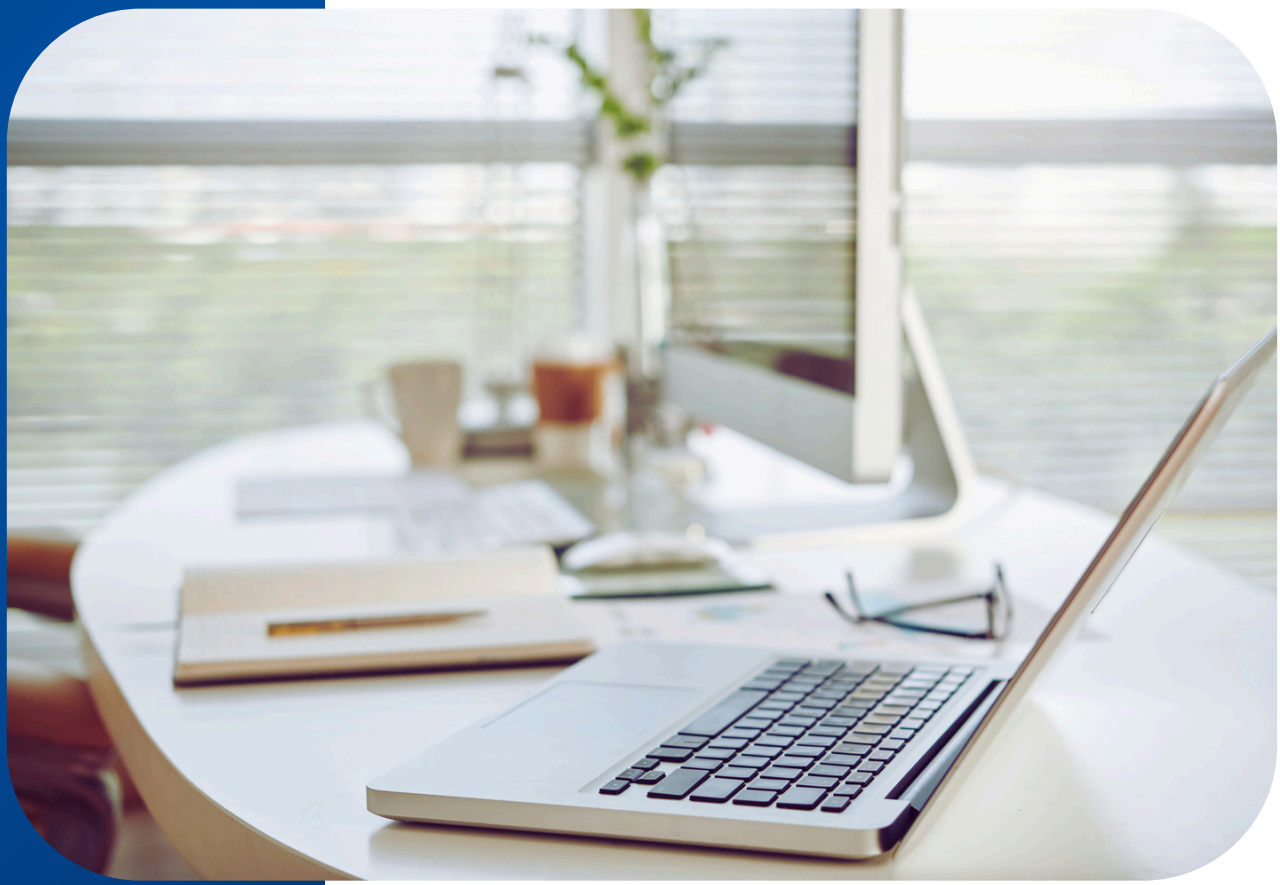
Clear Desk Policy



GENISTAR
Financial Freedom For All

Version Control

Version	Status	Description of Amendment	Date of Amendment	Amended By
V1	Inactive	Created	24/05/2018	Louise Skilton
V1.2	Inactive	Amended 4.2.1 and 4.2.2	07/09/2018	Louise Skilton
V1.3	Inactive	New doc template	05/03/2020	Louise Skilton
V1.4	Active	Reviewed and added to new template	22/09/2021	Kush Amin

Contents

1. Introduction.....1
2. Scope.....1
3. Purpose and Objectives.....2
4. Policy Statement.....2
- 4.1. Clear Desk Policy.....2
- 4.2. Clear Screen Policy.....3
5. Policy Compliance and Audit.....3
6. Reporting Breaches.....3

1) Introduction

Information is an asset. Like any other business asset, it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets.

Genistar is responsible for protecting the content of its documents and records, both in paper and electronic format. The General Data Protection Regulation (GDPR) requires Genistar to keep personal information secure.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure, and damage. By ensuring that users securely lock away all papers at the end of the day, when they are away at meetings and over lunchtime, this risk can be reduced.

Security risks of unauthorised access to electronic records are also prevalent when PC screens are left unattended.

Clear desks and clear screens also ensure that the Genistar projects a professional and efficient image to visitors, members of the public and colleagues.

2) Scope

This policy applies to everyone who has access to the Genistar's information, information assets or IT equipment. These people are referred to as 'users' in this policy. This may include, but is not limited to employees of Genistar, members, temporary workers, partners and contractual third parties.

All those who use or have access to Genistar information must understand and adopt this policy and are responsible for ensuring the security of Genistar information systems and the information that they use or handle.

This policy applies to all users whether office based or working remotely. The policy sets out Genistar requirements for each member of staff to protect any documents or records which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Emails
- Visual images such as work-related photographs
- Microform including microfiche and microfilm
- Audio and video tapes, CDs, DVDs and cassettes
- Genistar encrypted memory sticks
- Databases

This policy will also apply to any documents created in different formats in the future.

3) Purpose and Objective

The purpose of this policy is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them.

It is necessary to set out such a policy to ensure:

- The confidentiality, integrity and availability of information is adequately protected.
- A reduction in the risk of security breaches through theft of paper records or unauthorised access to paper records.
- A reduction in the risk of security breaches through unauthorised access to electronic records
- A reduction in the risk of damage to paper records by fire or malicious damage
- The presentation of a professional image of Genistar to visitors, members of the public and colleagues
- Compliance with the General Data Protection Regulation
- Compliance with Common law duty of confidentiality

4) Policy Statement

4.1. Clear Desk Policy

1. All users are to leave their desk/workstation paper free at the end of the day.

2. All users are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

3. Consideration should be given to the protective marking and sensitivity of information when storing it.

4. Documents which are likely to be needed by other members of Genistar should be stored in shared, locked filing cabinets.

5. Other documents may be locked in storage that Genistar provides individual users.

6. All office managers will have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

7. Users should make sure that any documents lying on their desk/workstation are not visible to visitors, members of the public or colleagues who are not authorised to see them.

8. Sensitive information, when printed, should be cleared from printers immediately.

4.2. Clear Screen Policy

1. All users are expected to log off or shutdown PCs/laptops when left for long periods and overnight.

2. When leaving their desk where it is no longer in their line of sight or, leaving your desk at any time when sensitive information displayed, users must always lock their Workstation.

3. Mobile devices through which access to the network can be obtained. These devices should be stored securely when not in use.

4. Users should make sure that no open documents on their computer screens are visible to visitors, members of the public or colleagues who are not authorised to view them.

5) Policy Compliance and Audit

1. Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the Disciplinary procedure, which may include dismissal. The Disciplinary procedure is part of the Local Conditions of Employment.

2. Non-compliance with this policy could have a significant effect on the efficient operation of Genistar and may result in financial loss and an inability to provide necessary services to our customers. Genistar will audit its procedures and where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other Genistar policies and procedures.

3. Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs. These will need to be risk assessed on a case-by-case basis.

4. It is the duty of all users to report, as soon as practicably possible, any actual or suspected breaches in information security.

5. Any user who does not understand the implications of this policy or how it may apply to them, should seek advice from their immediate line manager and/or the Business Integrity Department.

6) Reporting Breaches

Failure to observe the standards set out in this policy may be regarded as serious and any breach may render a user liable to action under the Disciplinary procedure, which may include dismissal.

All users have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Mitigate the problem from future occurrences

If a break is suspected, it must be reported to the Business Integrity Department at business.integrity@genistar.net

GENISTAR
Financial Freedom For All

Clear Desk Policy

GENISTAR LIMITED
Victoria House, Harestone Valley Road, Caterham CR3 6HY
Telephone: +44 (0)20 3372 5085
Authorised and Regulated by Financial Conduct Authority.