**Data Classification**

**Purpose**

This policy establishes clear standards for classifying data used or stored and the potential impacts of private data being exfiltrated.

**Scope**

This policy applies to all data stored or handled by personnel.

**Policy**

**Data Types**

* *Restricted*  - The highest privacy classification, restricted data has the most impact on if breached. Internal financial impact, and severe reputational impact.
* *Confidential -* Confidential data may include partner / contributor information. The impacts of a confidential breach include external (non-company) financial impact and moderate reputational impact.
* *Sensitive -* Sensitive data, if breached, will incur an impact on competitiveness in the marketplace.
* *Public -* Public data is information which is already viewable to the public and not subject to data access controls.

**Policy Compliance**

**Compliance Measurement**The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the Infosec Team in advance.

**Non-Compliance**

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

**Related Standards, Policies and Processes**

* Password Policy

**Definitions and Terms**

None.

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| **June 2014** | SANS Policy Team | SANS Template draft. |
| **July 2022** | Ivy Astrix | Initial draft. |