# Data Access Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

Information maintained by [Company Name] is a vital asset that will be available to all employees who have a legitimate need for it, consistent with [Company Name]'s responsibility to preserve and protect such information by all appropriate means. [Company Name] is the owner of all corporate data; individual units or departments may have stewardship responsibilities for portions of that data.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain quality. [Company Name] expressly forbids the use of corporate data for anything but the conduct of [Company Name] business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use. In addition, [Company Name] and its employees must comply with applicable state and federal laws and regulations.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

* This policy applies to all critical data in [Company Name], including data outside of [Company Name] stored in a cloud service. “Critical data,” in this context, includes email, personal and shared files, specific databases and web contents, and operating systems. The definition of critical data, and scope of this policy, will be reviewed on an annual basis.
* This policy applies to *staff* who may be creators and/or users of such data. The policy also applies to third parties who access and use [Company Name] systems and IT equipment or who create, process, or store data owned by [Company Name].
* This policy applies to data accessed from any computing device, including mobile computers, smart phones, and tablets.
* This policy applies to access of data persisted to mobile storage devices such as thumb drives, USB drives, SD cards, portable hard drives, etc.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **Private Data.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies [and other data as applicable].

**All information not otherwise classified will be assumed to be Private.**

Employees may not disclose private data to anyone who is not a current employee of the company.
2. **Confidential Data.** This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc.]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as applicable]. [Company Name] considers it a top priority to protect the privacy of our clients and employees. A separate privacy policy [provide link] outlines our commitment to protecting personal data.

Employees may only share confidential data within the department or named distribution list.
3. **Secret/Restricted Data.** This is defined as sensitive data which, if leaked, would be harmful to [Company Name], its employees, contractors [and other parties as applicable]. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes, but is not limited to audit reports, legal documentation, business strategy details [and other data as applicable].

Secret/restricted data cannot be disclosed by anyone other than the original author, owner, or distributor.
4. **Data Steward.** This is defined as a person who is responsible for managing data resources and enacting applicable data policies.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. [Access](http://its.virginia.edu/policy/admindataaccess.html#access) to Private, Confidential, or Secret/Restricted data by [Company Name] employees, employees of [Company Name]-related foundations, or non-employees sponsored by a [Company Name] manager requires that a formal request be made to the appropriate data security contact specifying the data desired and its intended use.
2. All data supplied as a result of a formal request may only be used for the purpose which was supplied. It may not be used for other purposes until an additional formal request has been made outlining these new purposes.
3. Individuals that seek permission to access data outside of the access plan and defined roles must submit a written request seeking non-standard access.
4. All requests for exceptions to data access policies must be made in writing to the data security contact. Email requests are acceptable. The request must specify the data desired and its intended use.
5. The data security contact must provide a written record of the reasons for denial of any request to access [Company Name] data. Email records are acceptable.
6. Employees, or manager sponsored non-employees, may appeal any decision that denies access to [Company Name] data. Appeals may be made to the appropriate data steward.
7. [Company Name] expressly forbids the disclosure of unpublished corporate data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the data owner. In this context, disclosure means giving the data to persons not previously authorized to have any type of access to it. [Company Name] also forbids the use of any corporate data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity.
8. Users will respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information. All data users having any access to Private, Confidential, or Secret/Restricted data will formally acknowledge (by signed data security policy statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data. Each data user will be responsible for the consequences of any misuse.
9. Users will comply with all protection [standards](http://its.virginia.edu/security/dataprotection/) for administrative data to which they have been granted the ability to view, copy, or download.
10. Users will be responsible for the accurate presentation of corporate data, and will be responsible for the consequences of any intentional misrepresentation of that data.
11. Users are responsible for notifying data stewards or data security contacts when they recognize that data is in error, incomplete, obsolete, or missing.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.