# Document Security 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.

# 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.

The purpose of a document security policy is to provide examples for document encryption redaction and metadata cleaning within [Company Name].

# 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 employees [check current definition of “employee” and list any other types of employees if necessary, e.g. contractors, casual workers, etc.] who work with our organization’s documents [specify scope of documents – just office productivity suites or other content as well?] in the course of their duties.

# Definitions

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

# 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.

[All documents/sensitive documents/ level [x] clearance] documents that are withdrawn from our content management system MUST be encrypted with [solution name] within [x] [hours] of their withdrawal [and/or] before transmission to [internal and/or external] stakeholders.

Encryption settings should utilize [specific encryption method and/or strength – provide a description of the relevant setting, for example, 128-bit encryption] using a password of [minimum character length – e.g. 8 characters] and a combination of alphanumeric characters. The password used for encryption must not be easily guessed – avoid personal details, interests, or other easily available identifying information when constructing a password.

[If your company or department requires the use of pre-approved or previously specified passwords, ensure the policy clearly states this here.]

[User-generated passwords in a private-key system should be sent over a secure channel to a duly authorized manager or IT representative to ensure documents can be retrieved in the event that the employee leaves the organization.]

Furthermore, [all documents/sensitive documents/level [x] clearance] should be set to allow access and editing only by the following user groups:

**Access:** [specify user groups]

**Editing:** [specify user groups]

### Document Protection – Redaction Policy:

[All documents/sensitive documents/level [x] clearance] documents that are withdrawn from our content management system MUST have the following information redacted prior to transmission to [internal and/or external] stakeholders:

[Enumerate a list here of material that is considered sensitive, and if necessary, specify if it is only to internal or external stakeholders, or both. Common examples include:]

1. Confidential financial information
2. Information pertaining to compensation and hiring practices
3. Trade secrets
4. Intellectual property
5. Product development information (i.e. blueprints/schematics)
6. Client lists or client records
7. Information on pending lawsuits or other confidential legal material

[Depending on the granularity of the information that needs to be restricted, each item on the list may require further enumeration.]

### Document Protection – Metadata Cleansing Policy:

[All documents/sensitive documents/level [x] clearance] documents that are withdrawn from our content management system MUST have the following metadata attributes purged prior to [transmission/publication/etc.] to [internal/external] clients or stakeholders:

[Enumerate a list here of metadata attributes that should be stripped from the document – a general rule of thumb is to leave those that add meaningful and useful context to the reader, but remove attributes that are extraneous or potentially damaging. Common attributes to be cleansed include:]

1. Individual author
2. Company Name
3. Date created
4. Date last accessed
5. Date last modified
6. Revision history
7. Comments
8. Geo-tagging or location-based information

Proper cleansing of metadata in [published documents] will be audited every [x] [days/weeks/months] by [responsible department or individual].

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# 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.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |