Template
Security and Privacy Standards

Provided by CSPO Tools - materials for the security and privacy officer

Highlights

Pre-written materials – ready for you to edit and use in your company.

Downloadable tools for self-assessment and compliance

Avoid the cost, and time, of building your materials from scratch.

Reduce your need for expensive consultants by using these materials

The cost? This document is free, and an annual subscription to our library of materials is only about equal to the cost of a book.

Stop by the CSPO Tools site to see what other materials we have available for you to use.

CSPO Tools, Inc.
Cary, NC
www.CSPOtools.com

Standardize your security and privacy practices

Creating a reference document for the standard security and privacy protections within your company is a key element in your overall information protection program.

It is much easier to work through the issues of such a document with an example in hand. CSPO Tools provides you with this template version, ready for you to use.

CSPO Tools also has a set of policy documents for you to use, so take a look at both documents. Just stop by the web site and download a copy.

You don't have to swim in circles, looking for security and privacy materials.

That's Delila, the company swan, in the picture at the top of the page. Some days she prefers swimming in the kiddy pool rather than the lake - she actually likes going round and round, getting nowhere.

But, you don't have to go round and round, getting nowhere, looking for examples of security and privacy materials. CSPO Tools has the materials you need already written, ready for you to download.

- Security and privacy policies
- Security and privacy standards for a company (more than just ths document!)
- Awareness training materials, ready for use with your staff
- Roles and responsibilities definitions, job descriptions – even pre-written job postings
- Self-assessment and compliance scoring tools
- Information security and privacy procedures
- Emergency response plans
- Compliance tools for PCI DSS, HIPAA, ISO 27000 series, FISMA, and more

We're adding more all the time, with many items free of charge. We invite you to stop by and see what is available – www.CSPOtools.com.

This is the template version of basic information protection standards for a company, provided by CSPO Tools, Inc.

How to use this document

Purpose

This is one of the standard documents which every organization needs to create. Since it is much easier to create this sort of document if you have an example in front of you, we are making this template version freely available to everyone.

In this document you'll find a set of security standards. These cover topics such as

- Default rules for passwords, timeouts, and similar issues
- Roles and responsibilities
- Basic rules for processes, such as awareness training, new employee hiring, etc.
- Basic rules for systems, networks, software, applications

In some companies these topics are called 'policies'. This is a word which confuses things – a 'policy' is also the word used for configuration rules at a detailed level, such as at a firewall. For this reason we have named this document a 'standard'. The rules (the 'policies') you implement on any particular platform may vary, so long as they meet this company standard.

Do you need 1000+ policy statements in your company?
Perhaps – but look at this document first. Often, a company sets out to create a pile of policies, when what they're really looking for is a standards document such as this one. If we called this document a collection of policies, it would be several hundred at minimum – and this one is free, so look at it prior to investing in anything more complicated or expensive.

This document fits into your company's overall security and privacy program:

- Your corporate policies (security, privacy, acceptable use, and the like)
- This standard
- An information architecture, which outlines what controls go where (on which platform, application, etc.)
- Configuration guidelines, for each platform or application

By the way - stop by www.CSPOtools.com to check for updates and additions to this document, and for other items (many are free, as this one is).

License

name, though – just use it inside your organization. (Yes, you may remove the header and footers once you've created your own version for use inside your company.)
Professional associations are encouraged to post this on their sites, so that everyone can easily find a copy.

Making this document suit your organization

We've worked with this kind of document at quite a few companies, and haven't yet noticed a pattern to how their documents are organized. In some companies, they try to organize the topics by such names as 'logical access', 'physical access', etc. In others, they try to organize according to the platform type involved – for example mainframe or PC, or according to the process underway (such as software development). So, we've organized this document in the most common manner, with major topics grouped together. You can consider how to organize those topics according to how people think and work within your company.

We did do one thing in this document, to avoid a common problem. Something to watch for in these documents is when you have a topic appearing the more than one place – if you update one occurrence, you still might miss the others. So, we've put cross-reference links within the topics, and have each topic only appear in one place. For example, the topic of 'backups' applies to many platforms, so we've just put a reference to backups under the platform sections, and then put all backup information into one place. That way, you can always find the standard for doing backups by looking at the topic of 'backups' – but you'll also find it if you are looking for PCs, notebook computers, servers, applications, etc.

Here's a more specific example:

- PCs (workstations) would require anti-virus, backups, change control, etc.
- A notebook computers section would refer to that same list – but would also include physical security items, to deter thefts
- Servers may not need anti-virus or anti-theft controls – but would still need backups and change control

So, we've put backups, anti-virus, physical security and such into their own categories, and have referred to each in the PC, notebook, or server sections as needed. That keeps each standard as occurring in only one place within this document.

As we release updates there will be more topics in our versions, so check back often to see if a new version is available for you to use. And let us know what you'd like to see in the next version of this document.

By the way, this template document doesn't have any graphics, backgrounds, or other fancy or fun stuff. That's because you'll be customizing it for your own use, and anything we put in you'd have to take out.

Optional text is marked in red. Whenever you see this red text, you'll have to fill in the blank or chose from several options.

As you read through this document, note the places where you may want to modify the defaults given. As examples:

- Do you want to lengthen or shorten the passwords?
- Do you want to change passwords more often?
- Do you want to make backups occur more or less often?
- Is the classification of information assets suitable for your company?
    - Do the titles suit your company?
    - Do you have more types of information, or are these classes sufficient?
- Are the roles and responsibilities suitable for your company's organizational structure?

Once you have worked out your updated version, make certain that all interested parties can agree to the new version. Your management, IT operations, along with your auditors and regulatory compliance teams will want to review the standard.

The sales pitch

This document is a part of a basic toolkit, which includes other policies, standards, and awareness training materials needed to start up the security and privacy effort at a company. The basic toolkit is distributed freely, without cost, in pdf format.

Subscribers to our library of tools have access to the source documents, in Microsoft Office or other formats as appropriate (this makes it easier for you to edit things), along with more tools.

For example: you may need slides and a script for you to follow when doing your awareness training for your employees… that sort of added tool is included in the library.

The cost is only about equal to a book – much less than the cost of hiring a consultant. Check in at our web site, and see what else is included in the library – we think you'll find there many more items which you can use.

■■■■

Please let us know if you need help, and what you would like to have added. We are at www.CSPOtools.com. And, remember – there's more free material on that site!

And now, onward to the template document…

<Company name>
Information Protection Standards

Covering security, privacy, and business continuity

Version x.xx

Date

Table of Contents

1 Change Control

Version	Date	Change summary
1.05	**July, 2009**	**Template version, provided by CSPO Tools, Inc.**

The master copy of this document may be downloaded from <your Intranet site>.

-OR-

Check with the Information Security team to ensure that you are working with the most current version of this document.

-OR-

Each version is effective for XX months after release.

2 Preface and background material

It is vital to the reputation and profitability of our company that our information, in all forms, be protected from unauthorized use, modification, loss, or copying. This document sets out the default standards which must be met to ensure that control.

Our information may exist on paper, in voice systems, on IT systems and networks, in the minds of our people, and in other forms. The information which needs protection includes, but is not limited to:

- Customer information (both for customer companies and for people as individuals)
- Financial information, including credit cards, salaries, banking, transactions and more
- Medical information of all types
- Company patents, business plans, and other intellectual property
- Company business records and planning materials, including our customer list, marketing and sales efforts, product line plans, and more.
- Copyrighted materials, both which our company creates and those which we obtain under license from others

Compliance with these standards is mandatory. Any deviation from these standards must be approved beforehand by the Information Security Officer.

2.1 Key concepts

Information Security Principles

The protection of information can be described in several key dimensions:

- Confidentiality
- Integrity
- Availability
- Provability
- Balance risk against cost of controls

In this document, the standards given are the company defaults. They must be applied where appropriate, but always balanced against the cost of implementing the control, and the value of the information involved.

Definitions: policies, standards, and guidelines

These terms are sometimes confused, so are defined here.

Policies are corporate documents which set out the company's position regarding business processes, behavior of personnel, and similar topics. Policies are a high-level statement of the company's position. Some of the company policies which relate to information security are:

- Information security policy
- Privacy policy
- Acceptable use policy for IT systems users
- Employment policies

These policies may be found <on our Intranet site> <in the HR department> <in the employee handbook>.

Standards are the rules which must be followed to enable an effective information security program. Compliance with the standards is mandatory, but deviation is possible if approved by the Information Security Officer.

Standards define the minimum, baseline procedures, practices, and configurations for systems, applications, controls, networks, and related topics. They are designed to provide a single reference point for use during software development and adoption, installation of systems and tools, and during the contracts process with vendors and service providers.

Standards do not, however, give detailed command-line instructions on how to meet the company's policies. Those are given in the *guidelines.*

Guidelines are built for each application and platform, and are the handbook to be followed when implementing that particular tool. So long as the security standards are met, however, a guideline may vary a bit from one implementation to another, so long as a justification is given and properly documented.

Put together, these three levels of documents provide a method for the company to audit itself and ensure that proper controls are in place, without excess cost or risk. They also provide a means for the company to explain to regulators, examiners, external auditors or investors how it is that our company is safe, trustworthy, and efficient.

3 Using these standards

3.1 Audience – who will use this document

This document applies to all of the company's business units, and also to all teams or companies supporting the company's business.

- Technology and business process providers should comply with these standards as a matter of contractual obligation
- Business units within our company should comply, unless a risk analysis has been done and a deviation approved by the Information Security Officer.
- Teams implementing technologies within our company should use these standards as a part of the requirements-setting process during the design of new tools and business processes

3.2 How the document is used

This standards document is a reference point for use by business units, technology implementers, and service providers to ensure a consistent framework of protections is in place. Implementing these standards involves:

- Review of existing controls, procedures, and tools against the standards
- Documenting compliance or deviations
- Gap analysis to determine where improvement are needed
- A risk analysis to validate that the improvements are justified against the costs of the controls and the value of the information involved
- Creation of a plan to close the gaps OR signoff of deviation
- Documentation of the new controls, procedures, tools

No signoff or approvals are needed if a level of protection *higher* that what is given in this standard is determined to be needed for a given information asset.

3.3 Exemption process – how to deviate from this standard

Steps in the exemption process:

- Documentation of the gap between the standard and the intended level of control
- Documentation of the *extent* of the deviation – one platform, one application, or all?
- Documentation of the value of the information asset involved. This includes both the asset value to the company, and also the regulatory/legal/market risk incurred if a problem does arise due to the reduced level of control
- Documentation of the intended, substitute protection method
- Review of this documentation by the business owner, and by the information security officer
- Publication of the new controls in the information security, audit, business unit, or other appropriate location

3.4 Maintaining this document

Periodic review and update

This document must be reviewed at least annually, and updates made to keep it in accord with the company's overall business goals and risk position. The review team should include

- Information security
- Auditors
- Legal
- Business unit representatives
- Company governance and compliance
- Human resources

Updates, suggestions, improvements

Any corrections, updates, improvement suggestion or other comments should be sent to the Information Security team at <email or Intranet site or intra-office mail address>.

3.5 Terminology used in this standard

Shall, Will, Mandatory, Must:

These words indicate that the standard mentioned is a requirement, and must be met.

Should, Recommended, Where Possible:

These words indicate that the standard mentioned is a preferred and accepted control. Deviation may be possible if compensating controls are in place, a risk analysis of the deviation has been done, and management signoff is obtained.

May, Optional:

These words indicate that the standard mentioned is optional. Deviation does not require signoff or approval, but is determined by the requirements of the implementation at hand. The implementation documentation should include a discussion of why the deviation was chosen, so that future reviewers will have all information needed.

4 Roles and responsibilities

4.1 Rules for ownership of information

The information and systems provided by the company to employees, contractors, trading partners and representatives are owned by the company, which also determines appropriate usage and access rules.

All data on the company systems and networks is owned by the company.

In this document, the words 'information owner' refer to the person who owns the responsibility for the information. The information itself remains the property of the company.

Each information asset within the company must have a designated owner.

4.2 The role of information owners

The 'information owner' is a business manager, in a business unit which generates or utilizes the information asset in question. The information owner

- Defines the appropriate levels of protection for the asset
- Classifies the information according to the company's classification standard
- Approves use of the asset, including copying, modification, access to, or destruction
- Is responsible for ensuring that the overall level of protection requirements assigned to the asset are in line with business values and goals
- Designates or approves the custodian of the data
- Assigns a backup person to cover the ownership role when needed
- Participates in risk assessments when controls over an information assets are being developed

4.3 The role of information custodians

Custodians of information are those who have the information in their care, either on systems, applications, or business processes. This includes those who operate databases, perform business tasks involving paper copies, and similar functions.

Custodians of information have responsibility for handling and protecting the information, but not for classifying it, approving access to it, or modifying it.
Custodians must maintain protections over the information in their care, and report problems or incidents.

4.4 Information users

Every user of company information must protect that information, and ensure that it is used for company business purposes only. Just as a person would not walk past a fire without reporting it, any incidents or questionable issues in the security of our information must be reported.

Information users may not assign access rights, authorize destruction or copying of information, or change the protections given to information assets.

Information users must comply with all laws, regulations, and company policies.

Clean desk

If you have a 'clean desk' policy, consider citing it here. For example:
<Users must comply with company policies regarding 'clean desks', ensuring that Confidential and Internal Use information is removed from their desk at the end of the day and properly secured.>

Clean screen

If you have a 'clean screen' policy for your workstations, mention it here. For example:
<Users must comply with company policies regarding logging off of unused workstations, called the 'clean screen' policy. >

-OR-

<Users must comply with the Acceptable Usage policy, including the 'clean screen' requirement to log off of all unused systems.>

4.5 Managers

Managers must ensure compliance with these security standards, and with company policies. Managers also are responsible for monitoring the activities of people, systems, applications, or networks under their control, to ensure that controls are properly met.

4.6 Information security officer

The information security officer for the company will

- Manage awareness programs relating to security and privacy topics
- Maintain a central record of exceptions to this standards document
- Manage changes to this standards document
- Provide leadership relating to new security risks, controls, and technologies

4.7 Privacy officer

The privacy officer oversees, and approves, the sharing and re-use of personally-identifiable information collected by, or processed by the company.

5 Information classifications and requirements

Information is classified to ensure that the controls applied to it are sufficient, and also to ensure that the controls applied do not impair the company's business, ability to compete, or the company's image.

All information must have a classification for security, and must have requirements set for business continuity.

5.1 The security classification process

Each information asset will go through this classification process. This includes, but is not limited to:

- IT platforms such as servers, mainframes
- IT applications, including databases, transaction processing, email
- Data sets
- Paper copies of information
- Information types typically known to employees, such as customer information

In general, an information asset includes both the raw information itself (paper, oral, data entry) the location where it resides, the business processes which handle it, and the systems and tools which handle it.

New information generated by the output of several information types must also receive a classification, since the new information may have a higher requirement than any of the separate inputs. As a default, the newly outputted information should have a classification equal to the highest of the inputs.

This classification review will be conducted by the information owner, with the participation of information security, audit, business processing, IT operations, and related teams.
<Consider setting a time schedule for getting this done.>
All information assets must be classified by <the end of year xxxx> <according to the attached schedule>
All assets will be reviewed at least once a year.

Information assets also will be reviewed during

- Development, acquisition, or deployment of software
- Connections of computers or networks to outside systems or networks
- Outsourcing of information processes, including IT systems and business processes
- Granting of access to outside organizations, including trading partners

Classification analysis structure

Information assets (data, platforms, applications, paper, knowledge, etc.) will be reviewed in several dimensions:

- Sensitivity: This refers to the value of the information if it is improperly disclosed, modified, copied, or destroyed. As an example, personal financial information is highly sensitive, since it should not be viewed by anyone who is not authorized. Keep in mind

that information can be highly sensitive even if you have backups of it – sensitivity refers to the overall value.

- Criticality: This refers to the requirement to have the information available when needed. Consider the loss if the information is not ready when needed, or is only partly available, and the difficulty in re-creating the information if it is not available.
- Legal and regulatory requirements: Some types of information have mandated protections which need to be applied, and thus the classification is already set out in the law or regulation. These include health care information, credit card transactions, online information about children, and other such topics.
- Market and customer expectations: Even if none of the other dimensions apply, is there an expectation on the part of customers or the market that the company will protect the information in a certain way? These can arise due to the company signing an agreement with a trading partner, or may be a part of the company's code of conduct or standing in an industry.

An ABCD structure will be used in evaluating each of these dimensions.

- 'A' refers to information which is critical, regulated, highly valued, or which will have a high impact to the company if the information is improperly lost or modified.
- 'B' refers to information which is essential to the company, in order to maintain product goals, quality, market position, etc.
- 'C' is for information which is important to the company, but which does not have an essential function in the business.
- 'D' is for information assets which meet none of these levels.

The security classification of an information asset is assigned according to the highest of these dimensions. As an example, if an asset is regulated by law, then it needs the highest classification, even if the asset is not critical to the company's business for any other reason.

5.2 The classes of information for security and privacy

The classes of information govern the gathering, creation, handling, copying, storing, usage and destruction of the information asset. It is the responsibility of the information owner to develop the classifications, and set the requirements for protecting the information.

The definitions of the assets classes are:

Confidential

This is the classification for information which holds a high value for the company, or for which there are legal ramifications if the information is disclosed or modified. This class of information is not generally known to outsiders, and may have economic value due to this secrecy. Loss or disclosure of this information would result in the loss of customers or markets, loss of prestige, loss of competitive advantage, or violation of regulation or laws.
Examples of this type of information include

- Business plans
- Company financial information
- Customer accounts
- Employee personal information such as salaries or health care

- Company decision rules or models
- Trade secrets
- Patentable work
- Engineering drawings
- Software being developed

Internal use

This is the classification for information which is of less value than Confidential information, but which the company still does not want disclosed to the general public or widely distributed without control.
This is the default class for any company information – if no other classification is assigned, all information is considered Internal Use.
This class of information includes items such as

- Company telephone books of personnel, jobs, titles
- Internal emails, except those which contain Confidential-level information
- Meeting notes, except those relating to Confidential topics

This class of information will be generally available to the employees of the company, but will require a non-disclosure or other agreement to be in place prior to having it leave the company.

Public

This class is for information which the company has designated to be available to the public at large, including;

- Information on the company web site
- Press releases
- Product or service brochures
- Advertisements
- Job opening postings

This class of information is assumed to be widely copied, but controls should be maintained to ensure that the information is not modified, and thus is correct when a member of the public accesses it.

Unclassified

<Consider whether you want this classification within your company – many of our clients do not use this one.>

Information which is known to be of low value or risk, and known to require little control, may be formally assigned the Unclassified category. However, information which is not yet classified is assumed to be Internal Use only.

5.3 Setting requirements for business continuity

The requirements for an information asset relating to business continuity are not set by classification, but are specific to that asset. They include:

- Required uptime for the information asset

- Required restoration time if the data must be restored
- Required frequency of backups
- Requirements for storage of backups
- Requirements for testing of the recovery process

A copy of the continuity plan for each asset will be stored with <Business Continuity team> <Information Security> <Audit>.

The default requirements for business continuity are listed in the 'information handling rules' section.

6 Handling rules for the information classifications

This section outlines the basic rules for handling information types, according to the classifications. More specific standards for platforms, processes, and networks appear in each topic section of this standards document.

6.1 Inventory of information assets

An inventory must be maintained of all significant information assets belonging to, or used by the company. This inventory must include:

- Asset name and characteristics
- The information owner
- The custodian of the information, and repository location (database, file cabinet, etc.)
- Asset value in dollars, or in other suitable measurement
- The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
- Requirements for the asset regarding availability, uptime, etc.

This inventory must be reviewed and updated annually.
Audit of the inventory will occur according to the company's audit schedule.

6.2 Rules for access to information assets

Vendors, contractors, and other outsiders

Any outside organization which wishes to gain access to Confidential or Internal Use information must

- Sign a non-disclosure OR
- Sign an approved contractual agreement
- Be willing and able to show that their controls are at least as stringent as the company's controls

Individuals

Individual persons who work for such an organization must also be bound to that outside organization's controls. Such individuals must

- Have a non-disclosure agreement with their own company OR
- Have a contract with their company
- Have appropriate background checks and bonding in place

By our company

Our company will not accept any confidential information belonging to third parties until that information is reviewed against our protections, and the appropriate agreements put into place and signed by the information owner. The agreements should include all requirements for controls over the third-party information, and the processes to be followed.

6.3 Rules, by security classification

Public information

This type of information does not require special marking or storage, except to ensure that it is available when needed. It does need to be kept safe from unauthorized modification.

Internal use

Access is granted on a need-to-know basis, as authorized by the manager of the user of the information. Some types of jobs are automatically granted access to data in this class.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes

- Printing this class of information only to a known, secure printer
- Encrypting or physically securing backup media
- Keeping paper copies of information locked or otherwise secured

This class of information is not released to anyone outside the company without a non-disclosure agreement, and without the approval of the information owner.

Internal use information must not be transmitted across any unsecured outside network or path without proper controls. Typically, this means encryption for files and emails, or secured packaging for paper copies. This information may be transmitted without encryption if it is masked or modified, so as to reduce its value from Internal Use to a lower level. For example, if all identifying information is removed from a transaction file, so that its loss would constitute no threat to the company, then the information may be transmitted over open networks without encryption. Such masking must be approved by Information Security.

Confidential

Access to this type of information is on a need-to-know basis, as approved by the information owner.

Copies of this type of information must have an appropriate notice on the document or media, stating that the information is confidential to the company and is not to be disclosed.

This class of information is not released to anyone outside the company without a non-disclosure agreement, and without the approval of the information owner and the appropriate business owner.

Confidential information must not be transmitted across any unsecured outside network or path without proper controls. Typically, this means encryption for files and emails, or secured packaging for paper copies. This information may be transmitted without encryption if it is masked or modified, so as to reduce its value from Confidential. For example, if all identifying information is removed from a transaction file, so that its loss would constitute no threat to the company, then the information may be transmitted over open networks without encryption. Such masking must be approved by Information Security.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes

- Printing this class of information only to a known, secure printer
- Encrypting or physically securing backup media
- Keeping paper copies of information locked or otherwise secured

6.4 Business continuity rules

Default rules

Backups will have the capability to back up and restore the operating system, applications, updates and patches, transactions, and data.

Complete backups will be performed once a week.

Fault logging will be enabled, in order to determine if errors occur during the backup process.

Incremental backups will be performed daily.

Critical information assets will have the backup data stored in a secured, off-site location.

Each asset must have a business continuity and testing plan.

Annual reviews shall be conducted by the information owner to validate the effectiveness and appropriateness of the business continuity plan for those assets.

In addition to the requirements for individual information assets, business continuity (contingency) plans are required for

- Data centers and networks
- Platforms which process or aggregate data
- Business processes which handle sensitive information, even without the use of IT systems

A continuity plan must contain

- A backup plan
- A definition of the systems, software, data, networks, and personnel to effect recovery.
- A definition of the backup locations of all required items. (For example, critical data would be off-site, backup systems would be at the backup site, etc.)
- A response plan for emergencies and incidents, to include recovery and restoration procedures, escalation and management notification, activation procedures for the plan
- A testing plan
- A plan for returning to normal operation once the emergency or incident is ended

Plans are to be tested at least annually.

Results of the tests are to be reported to <steering committee> <audit> <Information Security> <Business Continuity team>.

Rules for personal and mobile systems

Personal computers, notebook computers, mobile devices and PDAs are to be backed up by the user.
<Change this wording if you have an automated backup package in place for your PC and notebook computer users.>

-OR-

Personal computers, and network-connected notebook computers, will be backed up using the automated backup tool.
Mobile devices, PDAs, and other personal tools will be backed up by the user.

6.5 Retention rules for information

Information will be retained according to its sensitivity and to its business continuity requirements.

Default rules

<Set these rules to suit your company. Your legal department will have a large voice in setting these rules, since some retention requirements are controlled by law, some by contract, and some by any ongoing cases which you might have.>

Company financial information will be retained for seven years.

Email will be retained for 90 days.

Engineering, design, software, product development and similar information will be retained for seven years.

6.6 Disposal of systems and information

Information assets must be securely handled during destruction and end-of-life processes. This includes information on paper, on backup media, CD-ROMs and DVDr, and on the disk drives of all systems.

Secure containers will be provided for all users for use in the disposal of Confidential and Internal User information. The information placed into these disposal containers will either be shredded or otherwise securely disposed of.

No Confidential or Internal Use information may be disposed of in an office waste container.

An end-of-life for all systems, including notebook and personal computers,

- the disk drives will either be securely erased or the drive destroyed
- removable media will be removed and either destroyed, erased, or returned to the information owner
- ribbons and paper will be removed from printers and destroyed

Any systems which are leased must be securely erased of all company data prior to being retuned to the leasing company.

6.7 Information sharing and privacy

The sharing and re-use of personally-identifiable information is governed by law, regulation, and customer expectation. To ensure that the company meets those requirements, no personally identifiable information will be shared with outside companies, vendors, or personnel without the approval of both the information owner and the company privacy officer.

<If you don't have a privacy officer, designate someone to handle this issue. This is important! Many of the security breaches in the news are actually privacy breaches – no one broke into the company systems in many situations, but the company decided to share information, and still wound up in the news, and often in court.>

Personally-identifiable information includes

- Names
- Addresses
- Dates of birth
- Social Security numbers
- Ages
- Gender
- Personal financial information
- Personal medical information
- Personal buying histories

Aggregated and statistical data developed from this personal information is not still personally-identifiable, and thus does not need the approval of the privacy officer for sharing and re-use.

The company will comply with all applicable laws and regulations regarding the privacy of personal information, including such laws as

- Health Insurance and Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act
- COPPA – the Children's Online Privacy Protection Act
- International regulations, such as safe haven laws

Company employees, contractors, vendors and suppliers may come into possession of personally-identifiable information as a part of their relationship with the company. Each person must comply with all laws, regulations and policies and ensure that such information is properly protected.

6.8 Release of company information

Company information can only be released with the approval of the corporate communications team. This includes the posting of company information of any type onto bulletin board systems, public networks, news groups, or other open sharing tools.

Any information released must contain proper copyright, trademark, disclaimer, and patent notices as appropriate.

7 Risk analysis and management

Risks to the company assets and environment should be addressed proactively, rather than reactively. The controls applied to the risks must also be periodically reviewed, to ensure that the controls are working properly and efficiently.

7.1 Risk reviews

The job of reviewing risks, and setting requirements for controls, is a joint effort of the information owner, information security, audit, compliance, legal, and other control or advisory teams.
<The words above should reflect your company's actual organizational structure.>

Risks should be reviewed or assessed when

- Developing or deploying new applications, systems, networks, or software
- When significant changes are made to that same list
- When business processes change
- When the company enters a new geographical area of business
- When the company enters a new line of business
- Whenever the company does an acquisition, merger, or divestiture
- When incidents occur, or new risks emerge
- When new regulations or standards are set
- Whenever information handling or processing is outsourced

7.2 Risk management

Risks may be *accepted*, *avoided,* or *mitigated*.

Accepting the risk is appropriate when the cost of avoiding or mitigating the risk is greater than the expected loss. The losses considered should include the less tangible items such as reputation of the company, loss of market share, and loss of public trust in the company. Acceptance of a risk requires complete documentation of the risk analysis, and approval by the information owner.

Avoiding the risk is appropriate when the cost of insurance is less than the cost of incremental controls. Basic controls must always be in place, however.

Mitigating the risk is appropriate in most situations. These situations are those where compensating controls are possible, cost effective, and manageable. These mitigating controls may include

- increasing a protection to a level higher than what is listed in this standards document
- improving oversight or monitoring of the risk, to limit impact and minimize response time
- limiting transactions or other events to minimize the possible impact of the risk event

The method chosen for managing the risk (acceptance, avoidance, mitigation) must match the business value and costs involved, and must be approved by the information owner.
<Your company may have a steering committee, which approves this sort of risk management.>

8 IDs and accounts

8.1 User IDs

Each user shall be assigned a unique identification, called the UserID.
This UserID is not considered to be sensitive, unless the ID relates to an authentication process, systems or application management role. It may appear on business cards or in email signatures.

Where possible, the user ID should relate to the individual, to make it easier to identify the user. Use names where possible.

On sensitive systems or applications, the user ID should *not* be easily identifiable, to make unauthorized usage more difficult, since the user ID cannot be easily guessed.

Sharing of User IDs is not permitted, unless justified by business requirements and approved by Information Security. For any such shared IDs, the password must be changed immediately after the ID is used, to keep the shared ID from becoming generally available and a danger to the company.

Guest and anonymous IDs are not allowed, unless the system involved is not connected to any company network and the system does not have any company information on it. Typically, these guest or anonymous IDs are only used during development or during marketing/sales demonstrations.

Training IDs are to be used only for people attending a class, and when not permanently assigned to any person (only assigned for the duration of the class). These IDs must have passwords which conform to the general password rules of the company, which expire, and must be changed after the class is finished.

ID and account creation

User IDs are only to be created following a process approved by that information owner. This ID creation process should include:

- Expiration dates for the ID
- Renewal process for the ID
- Documentation of the role, business process, job function relating to the ID

User IDs are to be created for the purpose needed, and not in a manner to compromise segregation of duties.

IDs created for third-party users, such as contractors, should have a renewal time of no more than six months.

Users must acknowledge that they understand the conditions of access (usually a signature).
A record of all User IDs and their owners will be maintained by <Information Security> <the information owner> <the information custodian>.

Account suspension
User account must be suspended when inactive for 90 days.

Any ID which is not used within seven days of being issued will be disabled.

User IDs assigned to any departing employee will be disabled promptly.

Suspended accounts will be deleted within six months.

Information owners or their delegates must remove any user who no longer needs access to the information.

Account management
A periodic check will be made of all user IDs, and any redundant, dormant or unused IDs removed.

Information owners must review the privileges set up for user IDs at least annually.

8.2 Trusted accounts and IDs
Trusted IDs and accounts are used in support of automated applications, transactions, processes, or batch jobs. These have non-expiring passwords.

Trusted IDs must not be used by individuals.

Trusted IDs must be created only with the approval of the business owner, must be documented with Information Security, and must have strictly limited access rights.

Trusted IDs must not have *ad hoc* or interactive capabilities on the applications, systems, transactions or data involved.

8.3 Systems default IDs
Default IDs for systems, applications, software tools, and network devices must be changed upon installation, and must be disabled or renamed.

9 Authentication

All systems, applications, databases, or other information repositories shall require users to authenticate themselves prior to granting access. Authentication may be via an approved password scheme, or via an access control device, such as biometrics or a token.
The authentication method used must suit the value of the information asset, matching the cost of the authentication method against the level of protection required. In general, administrative and other high-value IDs will use the most secure methods of authentication – biometrics and tokens in addition to passwords.

A higher level of authentication may also be appropriate for remote access methods, such as dial or VPN.

9.1 Passwords

<Set these password rules to match your systems and business needs. For example, you might have a low-priority system which could safely use weaker passwords, or you might want to make the rules stronger for some high-value systems. It's ok to have a tiered structure for your password rules, to match the systems types.>

Format

Passwords must have

- A minimum of seven characters
- At least one numeric and one alpha character
- Not be composed of words easily guessed from a dictionary
- Not be the same as the user's name or ID
- Not contain repeating characters
- Not be constructed by any part of the user's name, telephone number, social security number, address, date of birth, business unit or location, or any other such information which is likely to be widely known

Rules

A maximum of three attempts will be permitted prior to disabling the account.
New passwords must be different from the previous three passwords.
Initial passwords issued for new IDs must be randomly chosen.
Passwords must be changed immediately upon first use of a new ID.
Passwords must never be stored or transmitted in clear text
Passwords shall be changed every 90 days.
Passwords for administrators and other privileged users shall be changed every 30 days.
Any passwords which are stored must be encrypted.
Systems must not echo back the password as it is entered.
Passwords must not be retained by any system or application longer than is needed to grant access.
Initial passwords must be transmitted separately from the ID.

Automated password resets

Passwords may be reset by automated systems so long as the systems implement a strong authentication challenge method, to include

- Verification of the user's date of birth, or other personal information
- A correct response to a preset challenge question
- Personal or business information which would be known only to that user

9.2 Authentication devices

Administration of these devices shall be considered a high-value, high-risk role, and all information relating to the configuration and operation of these devices shall be classified as Confidential.

Biometrics

Biometric devices need to have expiration dates on the authentication method.
Biometric authentication methods should have a backup method in place, for use should the user be injured or otherwise unable to use the device.

Tokens

The selection of authentication tokens, such as challenge-response cards or key fobs, shall be done by the Information Security team. Approved devices will be published in the security architecture document.

10 Authorization and rights management

10.1 User types

Each information asset or repository will have standard user types:

- Information owner
- Information custodian
- Systems or application or platform administrator
- Information user (may be many types of user)
- Manager of information users (might not be the same as the information owner)
- Help desk or other support staff for the users

The information owner will develop the access rules, usually in a matrix or list format, controlling access for the user types.

10.2 Access rules

User IDs and accounts must be authorized to access only those elements needed for the user's role, including

- Limiting access to datasets and types
- Limiting access to operating systems
- Limiting transaction types, frequencies, or amounts
- Limiting times of access

Access to operating systems, *ad hoc* transaction capabilities, software development tools, and other systems devices must be controlled and limited to only those user IDs which require that access.

Segregation of duties shall be established for all information asset controls, to minimize the possibility that one person is responsible for an entire asset.

A user (and hence user ID) which changes role or job function must have access rights updated to match that new job function or role.

Systems and applications will have an automatic timeout for inactivity:

- High value or high-risk systems and applications will have a ten minute timeout
- Normal, medium-risk applications or systems will have a 30 minute timeout
- Low risk systems need have no timeout implemented

10.3 Privileged users and accounts

Privileged users are defined as those who

- Have any control over security tools on an application, system, or network
- Can update operating systems or similar tools
- Can directly modify data within a database or application

- Have any special capabilities built in by the vendor of the application software, operating system, or platform

Access at a privileged user level shall be granted only on a need-to-know, need-to-perform basis, and then only to the assets required.
Privileged user access shall only be granted to those supporting the company applications, networks and systems.
An audit trail shall be maintained to make it possible to review the actions taken by privileged users.

10.4 Emergency accounts

These accounts are used as a failsafe measure, for situations where all normally-authorized administrators are unavailable or cannot make access.
Any emergency accounts shall

- Be created only with the approval of the information owner and Information Security
- Be stored in a secured location
- Have the use of such an account recorded and approved
- Shall have the passwords for any such accounts reset after each use

11 Information security administration

The administration of security tools (IDs, passwords, authentication devices, rights management) is a high-value role for the company. Persons assigned to this function must pass appropriate background checks.

The responsibilities for security administration for each asset shall be assigned or approved by the information owner.

Persons performing the security administration tasks will not have access to the applications, systems, or networks involved, but will have access only to the security tools.

All actions of security administrators will be logged, and periodically reviewed.

Logs of security administration activities will be retained for one year.

Security administrators are accountable to the information owners for the actions taken.

Security administrators are responsible for compliance with all company policies and standards.

12 Incident response and reporting

12.1 Incident definitions

An incident is defined as any breach of security, privacy, continuity, legal or regulatory controls over information assets of any type. Examples of such incidents include

- Penetrations of systems, applications, networks, databases
- Denial of service attacks
- Misuse or mishandling of assets
- Virus or other malware contamination
- Transaction errors
- Breaches of confidentiality agreements or contracts
- Legal or regulatory violations

12.2 Incident reporting

The company will maintain an effective method so that all information users, custodians, and owners can readily report incidents.

<Recommended:
Incidents will be reported to the security hotline, and will be handled by the Information Security team.
-OR-
Incidents will be reported to the person's immediate manager, who will then notify the Information Security officer.

Periodic summaries of incidents will be made to <the steering committee> <the risk management committee>.

Reporting theft of equipment

<You may want to have a separate reporting method for thefts – perhaps to your physical security team, rather than to Info Security.>
Theft of equipment or information shall be reported to Information Security.

12.3 Incident response

The Information Security team will investigate incidents, and will report significant losses or threats to the steering committee immediately.

Incidents involving misuse by employees will be turned over to Human Resources for investigation.

13 Personnel security

13.1 Newly hired personnel, third parties, vendors

Personnel screening

Proper verification checks must be made prior to granting any new employee, contractor, vendor, agent or affiliate access to Confidential or Internal Use information. These verification checks will meet the requirements set by the company's human resources department, and may include

- Professional qualifications
- Identity checks
- Criminal checks
- Confirmation of academic and professional experience

The information owner is responsible for ensuring that these checks are made on parties who are not newly hired employees.

Terms of employment

Compliance with company policies regarding security and privacy are a condition of employment.

Acknowledgement

All users shall be required to sign an acknowledgement after being briefed on the company's security and privacy policies.

13.2 Exit process for users

Upon exiting employment or any relationship with the company, all users who have been granted access to any information asset shall

- Relinquish all access control devices
- Report all user IDs in use by the person
- Relinquish all information stored, whether on paper or on backup media
- Relinquish all information processing devices, including notebook computers, workstations, mobile devices and others

13.3 Ongoing training

An ongoing training program shall be established for all users of company information assets. Training shall occur at least annually, and also during the process of granting new access to users.

Some of the topics which the training shall cover include

- The policies, standards, and procedures of the company
- Requirements governing user IDs and authentication methods
- Practices relating to clean desks, logout when not in use, etc.
- Best practices in protecting PCs, notebook computers, mobile devices
- How to report an incident or risk
- Awareness of social engineering, phishing, and related scams

- Policies and guidelines governing use of the Internet and company email
- Compliance programs
- Monitoring of usage on systems
- Laws and regulations
- Security efforts underway at the company

13.4 Disciplinary processes

Failure to comply with the company's policies or standards shall result in disciplinary actions, which may include termination of employment or of the relationship with the company.
The disciplinary process shall be handled by the company's Human Resources department, in accordance with <the Code of Conduct> <company employment rules>.

14 Legal and regulatory issues

14.1 Legal processes

Responses to subpoenas, deposition requests, and other legal issues will be referred to and handled by the company legal department. IT managers, systems and application developers or operators are not to respond to such legal processes without company legal counsel.

14.2 Notices

Logon banner

All systems will have a warning banner at login, which will state:
<Have your company legal counsel approve this login banner.>

The information on this system is confidential, and is proprietary to the Company.
Access to this system and network is limited to those approved by the Company.
The Company will monitor all uses of information, applications, and systems.
No information may be copied or sent out of the Company systems or networks without prior approval.
Use of this system constitutes acceptance of these terms.

Email signatures

Outgoing email messages must have a signature containing a disclaimer and notice, approved by the company's legal department and by Information Security.

<Update this version to suit your company.>

> The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. If you are not the intended recipient, any copying, use, or distribution of the information in this email is prohibited and my be unlawful. The Company disclaims all responsibility and liability for information contained in this email and attachment.

14.3 Copyrights and licenses

The Company may have agreements in place governing the use and handling of software, information, and other tools which are owned by other entities.

All users and information owners will comply with those agreements.

A copyright notice must be placed onto all software developed by the company.

Users are responsible for complying with copyrights regarding any material obtained via the Internet. This includes files, graphics, software, audio and video materials.

Users may not agree to a new copyright license, unless given permission by their manager.

Licensed software must be used in accordance with the license agreement, and only the number of copies licensed must be created or used.

14.4 Export controls

Information may not be exported across country boundaries without prior approval of the company's export control officer.

<Designate someone for this role – usually it's legal counsel if no one else.>

15 Malware

Data entering the company systems and networks must be subject to an up-to-date anti-virus scanning tool. This includes emails, attachments, disks, backup media, USB memory devices and other data carrying tools.

Data entering the company systems and networks must also be subject to an up-to-date tool which scans for Trojan Horse malware and any other threats which arise.

Data exiting the company should be scanned for viruses and other malware. This includes emails and attachments.

All company employees, affiliates, contractors, consultants, vendors, representatives or other service providers must make certain that adequate controls are in place to guarantee that data coming from their systems and networks is free from malware.

Users of company systems, applications and networks must not create, copy, or propagate any software which may harm the assets of the company.

The company will use approved tools to monitor and remove malicious software from company assets.

All portable media must be immediately scanned when attached to any company device.

All devices such as notebook or other portable computing systems must have anti-malware tools in place prior to being connected to the company networks.

16 Audit logs

16.1 Requirements setting

The requirements for audit logs shall be set by the information owner, with the approval of < information security, audit, and the steering committee> OR <the risk management committee>.

The exception to this is that all systems and tools involved in the protection process are required to always have audit logs enabled and properly configured. This includes

- Firewalls
- Email servers
- Anti-malware tools, especially the administration tools
- Access control tools
- Security administration tools, such as password resets and account modifications
- Monitoring tools
- Routers and other network devices

16.2 Audit log rules

Audit logs must be retained for at least one year in raw format, preferably electronic, to preserve evidence.

Audit logs must be configured to prevent overflow, erasure, or tampering.

Audit logs will be configured to record information such that:

- Sufficient information is available for proper investigation of use, misuse, incidents, and performance
- User ID, event type, date and time are maintained.
- Time is according to a known time stamp, so that events across systems can be coordinated
- End-to-end accountability is always maintained

Events to be recorded include:

- Login attempts
- Resource request failures
- Login and activity by any other privileged accounts
- Unauthorized attempts to modify or delete information
- Changes to operating systems, application code, or other tools
- Security administrator activities
- Systems administrator activities
- Backup and restore events
- Changes affecting any cryptographic keys or devices
- Changes to clocks
- Stop or start of critical processes
- Transaction failure, re-try, duplication

16.3 Analysis of audit logs

Audit logs will be reviewed and analyzed by delegates of the information owner, or by Information Security.

Reports on problems and incidents will follow the incident reporting method, listed elsewhere in this document.

17 Encryption management

The implementation of any encryption scheme must meet the approval of the information owner and Information Security.

Deployment of the encryption tool, including all keys, must meet industry best practices and be properly documented.

Encryption keys will be managed by Information Security.

International laws must be considered before deploying any encryption tool.

17.1 Network encryption devices

Use of these devices may be necessary to protect data as it travels over public or otherwise unsecured networks. The use of software-level encryption tools is preferable, since these are more adaptable.

The use of these devices shall be documented and approved by Information Security.

Key management for these devices shall include:

- Encryption keys for link-level encryption devices shall be changed from default prior to installation
- Link encryption keys must be changed quarterly
- Key management processes must be documented
- Audit logs must exist to cover the changing and handling of encryption keys
- Encryption keys must require at least two people to be involved in the change process
- Physical keys must be secured as high-value devices

18 Vulnerability assessments and penetration tests

Vulnerability and penetration tests will not be conducted except with the prior approval of Information Security.

No user will have vulnerability or penetration testing tools loaded onto any company system without prior permission from Information Security.

18.1 Penetration testing

Penetration testing will be conducted annually on all networks and on critical systems.
Testing shall validate the security of

- External connections
- Operating systems
- Applications
- Databases
- Network controls
- Security procedures, including monitoring and incident response

18.2 Vulnerability assessment testing

Vulnerability assessments will be conducted annually on all network-connected systems devices. Any vulnerabilities found must be corrected in a timely manner.

Vulnerability assessments also shall be conducted when:

- A new system, application, or network is installed inside the company
- Changes are made to firewalls, VPNs, or other security control tools
- Changes are made to a web server's operating system
- Changes to email servers
- Configuration changes to databases
- Configuration changes to critical applications

18.3 Remote access testing

Dial access

Testing of dial access points (war-dialing) shall occur regularly, to cover all telephone numbers assigned to the company.

Wireless access

Testing of wireless access points (war-driving) shall occur regularly, to cover all wireless access points under the control of the company.

18.4 Password testing

Password cracking software shall be run periodically to validate the enforcement of password rules.

19 Use of email, Internet, messaging, public sites, blogs

Confidential and Internal Use information must not be transmitted across any unsecured outside network or path without proper controls. Typically, this means encryption for files and emails, or secured packaging for paper copies. Refer to the 'handling rules' section for detailed rules controlling the movement of company information over these types of external connections.

Users are responsible for ensuring that their use of these tools complies with all company policies, and with applicable laws and regulations. This includes all employment policies such as sexual harassment, stalking, ethics, and appropriate use.

These tools may not be used to access, send or receive, store, or display

- Sexually explicit material
- Company confidential or Internal use material, except as meets the 'Handling Rules' section
- Viruses
- Threats
- Inappropriate or unlawful language, including
    - Offensive language
    - Language inappropriate for the company environment
    - Discriminatory or harassing language
- Tools usable for hacking, password cracking, vulnerability scanning, penetration testing

Use of company-provided email, Internet or wireless access is for company business. Incidental personal use is permitted, provided that such use does not interfere with company business or the performance of the user's job function.

These tools are the property of the company. Access may be unavailable at any time, at the company's discretion. User must not assume that access to these tools will be available for incidental, personal use.

All content transmitted over these tools is the property of the company. Content, including emails, may be inspected by the company. Such inspections will occur with the approval of Information Security or of the company legal department.

The company may monitor, filter or block content on these tools.

Users of blogs, public affiliation site such as Facebook, and other such tools must not represent their comments as coming from, or being representative of, the business or opinions of the company.

20 Workstations, PCs, notebooks, mobile devices

Workstations are devices which are at company locations, and thus have some level of physical security. These devices still are easily attacked, and thus must have access controls and anti-malware as specifies in those sections of this document.

PCs, notebook computers, and mobile computing devices are considered to be high risk since they are often operated in locations which are not physically secure, and they are easily attacked by hackers or others. Therefore, a high level of protection is required over these devices.

Users of these devices are required to ensure that all appropriate protections are in place, including

- Physical security to prevent theft or misuse
- Access controls suitable for the class of information on the device
- Anti-malware
- Keeping the devices locked to a desk or other secure location when outside the company
- Keeping control over backup media, so minimize the possibility of theft or loss
- Ensuring that the transport of these devices is secure, and is safe from damage. For example, these devices should only travel in padded containers, and should be locked and shut down during transit
- Keeping all operating systems and tools up-to-date, with all updates and patches.

Specific requirements for these topics are in the appropriate sections of this document.

Company devices must not be used by people who are not authorized, including family members and friends.

Software loaded onto such devices must follow the rules in the 'Software' section of this document. In general, only approved software may be loaded, and shareware, games, and other such software are not permitted.

International travel with these devices may require special approvals or configurations, especially as regards encryption and licensed software. Before traveling internationally, contact Information Security to determine if such special considerations exist.

Use of these devices for remote work, including telecommuting, must be approved by the information owner and Information Security.

Connecting these devices to company networks must follow the rules in the 'Networks' section of this document. In general, all such devices must be approved prior to connecting.

The business manager is responsible for maintaining an inventory of these devices, including serial number, user name, and normal location for the device.

Devices of these types which contain Confidential information must have disk-level encryption in place, as approved by Information Security.

If these devices are to be shared-use, then a separate login ID should be used for each user, rather than a single, shared login ID.

Remote access from these devices to company networks and devices must meet the controls specified in the 'Network' section of this document. In general, such access must be approved, and must have adequate controls over the security of information in transit.

Devices of these types which are owned by contractors, vendors, or other third parties must meet all company requirements prior to being connected.

21 Networks

21.1 Operations and management

Company networks and devices must be designed, deployed, and operated in a manner so as to provide proper levels of protection for the data being accessed and transported.

Significant changes in network designs must be piloted before deployment.

The types of devices and networks used must follow the approved list from Information Technology Operations and from Information Security.

Mechanisms must be in place to alert network operators and administrators of possible attacks and breaches, to include

- Denial of service attacks
- Improper access
- Virus infections
- Unauthorized software installations, email, FTP or other improper usage

Analysis must be conducted at least annually to validate the failure mode and recovery for all devices, network circuits, and protocols.

Responsibilities must be defined for

- Administration of network and communications connections
- Operations of all devices
- Monitoring
- Timely review of audit logs, and response to alerts or alarms
- Review of unusual patterns of usage or activity

To minimize risks, any network connections or network segments should be disconnected when not in being used.

Monitoring

The use of intrusion detection, usage monitoring, and change monitoring tools such as sniffers, protocol analyzers and scanners must be approved by Information Security.

Protection devices on the company networks, such as firewalls, will be operated to industry best practices, including daily reviews of alarm and alerts.

Diagnostic information such as data dumps and traces are considered to be confidential information, and must be protected so as to avoid leaking information about security controls on the network.

Access control and physical security

Sites where company network equipment or communications lines exist are considered to be high-value, and thus are subject to the access control and physical security rules outlined in the 'Computing Center' and 'Physical Security' sections of this document. In general, these rules will require

- Access be limited to authorized personnel only
- Physical security, including locks, be in place
- No shared access locations be in use.

< Here's an example – do not allow your network devices to be in a closet where the janitor also stores wet mops. Sounds silly – but we've seen more than one problem of this type, especially in sites which are smaller and far away from the company headquarters.>

21.2 Change control

New connections

Designs for new connections must have approval from the Information Security team.

Connections between company networks and third-party networks will require appropriate legal agreements, including non-disclosures.

Modifications, updates

Changes to the network architecture which affect the protections must be approved by Information Security. Examples of such changes include firewalls, wireless configurations, port and proxies.

21.3 Documentation

The network operations team shall maintain an accurate set of document of the networks and their components. This documentation is considered to be highly valuable, and so will be Company Confidential.

21.4 Network design

The goal for network design is to facilitate the company's business, while still providing protection for company assets.

Segmentation

Company networks will be segmented as practical in order to limit access to Confidential information, without impacting the company's business. Intranet firewalls and other tools may be appropriate to control the Confidential sections of the company networks.

Firewalls

A security boundary will be maintained between the company networks and any external network. This typically would consist of a firewall server, router, or gateway. Such devices and designs will be reviewed by Information Security. These boundaries will exist to protect

- Access from the Internet to company networks

- Access from company networks outward to any external network
- Connections between company networks and third-party networks, including those of trading partners, including companies and government agencies

Firewalls will isolate company networks with are operating at differing levels of security.

Disclaimers and warnings

Entry points to company networks must display a disclaimer and warning banner as described in the 'Legal and Regulatory' section of this document.

Internet

Connections to the Internet must

- be approved by Information Security
- be periodically reviewed and tested for vulnerabilities
- be protected by firewalls, intrusion detection systems, and anti-malware tools

Some Internet tools, such as FTP, IRC, Telnet, and RPC are restricted in use, and must be approved for use by Information Security.

VPN

Virtual private networks (VPNs) will be used for traffic flowing over public networks, to ensure the proper level of protection over company data.

Wireless

Wireless connections must have a robust security architecture, which must be approved by Information Security.

Dial

The use of dial connections is discouraged.
Any dial connections must have a robust security architecture, to include

- two factor authentication of users
- where possible, a dial-back arrangement
- no permanent connections of modems to network devices or other high-value devices
- dial-out modems must not be set to auto-answer
- use of firewalls

Use of dial connections must be approved by Information Security.

Local area networks

The administrator for the LAN shall be responsible for

- operating and maintaining anti-malware tools
- security administration of file/print devices
- monitoring for security breaches

<Adjust these roles to suite – you might have the InfoSec team do the monitoring, for example, if you have a sufficiently strong central tool in place.>

Devices such as secure hubs should be used to prevent eavesdropping of packets or masquerading of port devices.

22 Distributed systems, servers

Systems, applications, and devices in a single distributed environment must all operate at the same level of security and protections. If varying levels of controls are to be in place, the distributed systems must be protected with a network firewall as described in the 'Networks' section of this document.

Client-server systems must be able to provide an end-to-end audit log for all transactions and security events.

23 Computing centers

Computing centers are defined as locations where there is a significant concentration of systems, servers, processes, or networks. These centers are considered high-value, and must have controls to suit that value, including

- Physical security and environmental controls as defined in the 'Physical Security' section of this document
- Audit logs as defined in this document
- Backups and business continuity plans
- Proper access control over users
- Proper change control
- Documentation of authority over changes, security tools, monitoring tools

Computing centers must have proper controls of the contents of media library materials. These include

- Controlled access to media
- Accountability for media movement, including arrival, usage, exit, disposal
- Semi-annual inventory of media
- Proper labeling of all media, including sensitivity and classification
- Media retention rules

24 Physical and Environmental Protections

Physical and environmental controls are assigned according to the sensitivity, value, and threats to a given site or asset. These controls are designed to protect against theft, intruders, weather events, loss of power or cooling, and similar threats.

Critical assets and operations must be conducted in a secured area or secured site, with protections implemented in accordance with the risks and value of the assets, information and operations.

24.1 Definitions

Secure sites

These are locations which require the highest level of protection. These sites include

- Computing centers
- Network connection points
- Media storage locations
- Locations containing platforms which carry high-value or critical information or transactions.

Secure areas

These may occur within company buildings, where the overall building is operated to a lower level of security, but a certain area is more controlled due to documents, assets, or processes which occur in that area. A set of controls, such as locked doors and badges, would define the boundary between the overall site and the secured area.

Vulnerable devices

These include notebook computers, PDAs, wireless devices, and other tools which are used outside of sites where the company can provide physical security.

24.2 Secure sites

Secure sites shall be established for all computing centers, and other locations where there is a concentration of high-value or sensitive information, systems, or networks.

Sites will be designed and operated according to best practices, and in consideration of threats appropriate to the site such as hurricanes, tornados, power outages, and intruders.

This Standard is not to be construed as a complete list of requirements for a secure site. It should be used in conjunction with expert advice, architects, fire marshals, OSHA and other regulations.

Site design

The site shall not be located in areas prone to disasters, including any high likelihood of

- Hurricane
- Tornado
- Social unrest
- Loss of power

- Chemical contamination
- Explosive or other industrial accident

Separate, isolated areas will be created within the secure site for

- Media libraries
- Electrical supplies and controls
- Environmental controls
- Mechanical controls

Access to these sub-areas will be on a need basis.

The external walls of a secure site should be brick or reinforced concrete, so as to resist physical attack.

Windows at ground level should be strengthened with grilles or with impact-resistant glass.

Sites should be designed for ease of reparability and relocation.

Operations

Equipment moving into or out of a secure site must be properly authorized and inventoried.

Alarms shall be in place, operational, and tested regularly.

Access to secure sites shall be restricted to those requiring entry to the site to perform their job functions.

All persons entering or within secure sites shall wear badges or other identification devices.

Visitors shall sign in and out of the site.

Loss of any access control key or badge must be immediately reported.

Physical control over access

The location of the secure site shall not be made public, including by signs outside the building.

Access to the site shall be by badge or by other approved control. These badges shall be under dual control, shall be strictly inventoried and controlled.

Emergency exits should open outward, be marked for emergency use only, and be alarmed.

Guards should monitor or patrol the site during after-hours times.

Fire protection

Fire protection shall meet all regulations, including federal, state and local.

Operational areas within the secure site must not be used for eating, drinking, or smoking.

Work areas are to be kept clean, with no build up of combustible materials.

Automatic fire protection, detection, and suppression systems will be in place and operational.

Fire extinguishers shall be deployed in accordance with regulations of OSHA and fire inspectors.

Periodic testing of alarms, fire extinguishers, and fire evacuation procedures shall be conducted.

Environmental controls

Water detectors shall be installed under raised floors, and connected to alarms.

Backup air-conditioning, UPS, and power sources shall be installed according to the needs of the site.

Temperature and humidity shall be monitored.

24.3 Secure areas

Secure areas will be established within company buildings when sensitive or high-value information is being handled, stored, or processed.

Physical control over access

Access to secure areas shall be controlled, and restricted to authorized personnel.

Secure areas will have a physical access control method to delimit the area from the overall building. Some methods by which this may be accomplished include

- Doors with badge access
- Guard facilities to govern access
- Doors with buzzer access

24.4 Vulnerable devices, including notebooks, PDAs, wireless

Users of vulnerable devices such as notebook computers, PDAs, and wireless devices must physically security these devices whenever they are outside of a company secure area or site. This can be done by

- Locking the device in a disk or cabinet
- Putting the device into a locked docking station
- Using a cable lock to secure the device to a desk

The use of full-disk encryption on these devices will greatly reduce the liability for any information lost, should an event occur.
<Consider mandating this encryption for your notebook computers!>

25 Software

This section outlines the standards applying to operating systems, applications, databases, and other software tools.

25.1 Acquisition

Management approval must be obtained and documented to authorize the acquisition of software.

Software must be screened for malware prior to being installed.

Any unauthorized, illegally acquired, or unlicensed software must be removed.

Users of workstations, notebooks, wireless and other personal devices must not install games or other unapproved software.

Shareware, freeware

The use of shareware or freeware may only occur if

- It is not used in a production environment OR
    - It is fully tested, documented, and company personnel assigned to support it, prior to it entering a production environment
- It is downloaded from a known and trusted source
- It is immediately checked for malware, back doors, and other vulnerabilities prior to use
- Source code is examined in detail prior to use
- The business owner, information owner, and Information Security teams approve of the use

25.2 Documentation

Documentation for sensitive applications and the operating systems which run those systems shall be stored securely.

Backups of all documentation shall be maintained off site.

Access to the documentation for sensitive applications and the operating systems will be on a need-to-use basis.

25.3 Software Development

Requirements for software, either acquired or developed, shall include information protection.

The software development lifecycle shall include protection testing and validation at the appropriate stages. For example, at integration test and user acceptance testing stages.

Protection requirements testing shall also occur if software is significantly updated or changed.

The requirements-setting process shall include participation by information owners, legal/regulatory compliance, and Information Security.

Testing shall not occur using production data. All test data shall either be anonymized or otherwise sanitized to prevent the leakage of customer, company, or client information.

25.4 Change control and maintenance

All change and maintenance processes shall include testing and validation that no security vulnerabilities have been introduced into software, including malware, back doors, violation of access rules, or other problems.

25.5 System Software

All IDs and accounts provided by the system software vendor shall be removed or renamed.

System software must be tested to validate the information protections prior to implementation.

If the native security of a system software package is insufficient, added security tools must be installed or the software must be rejected.

Changes and additions made to vendor-supplied systems software must be fully documented.

Systems programmers must not have access to the data or application code in the production environment, but must test in a clean test environment.

Operating Systems

Standardized operating procedures must be developed and used for installation, configuration, operation and maintenance of operating systems.

Default settings must be reviewed prior to installation, to identify any security vulnerabilities.

Operating system services which are not needed should be removed from the system. This includes

- Command-line or other direct entry capabilities
- *Ad hoc* query capabilities
- Development tools, such as compilers
- Unused services such as FTP, IRC, etc.

Administrator, maintenance, and guest accounts must be deleted or renamed.

Auditing must be enabled.

25.6 Applications

All applications, whether developed or purchased, must comply with company policies and protection standards.

The information owner is responsible for ensuring that these requirements are included during the development or acquisition of software.

The protection requirements for applications include

- Access control
- Authorization
- Information classification
- Storage controls
- Backup and restoration
- Confidentiality and integrity requirements
- Audit logs
- Privacy, export control, and other such requirements

Single sign-on should be implemented where possible.

Blank documents (such as blank checks) must be controlled as a part of the implementation process for applications.

25.7 Databases

Related rules are in the Audit log, Backup, Access control and in other sections within this document.

Access to databases will be by approval of the information owner only.

All information which is to be shared must be within a data dictionary, and be assigned to an information owner.

Administrator and guest accounts must be deleted or renamed.

Audit logs will be enabled.

Security-related patches will be applied as soon as practicable.

26 Appendix – information classifications already known

Some types of information are already classified for you, either by law, by industry standard, or by customary practice. Here are a few:

Asset	Confidential	Internal Use	Public
Credit cards and transactions	XXXX (by industry standard and laws)		
Employee health care information	XXXX (by law)		
Online information relating to children under 13	XXXX (by law)		
Company business plans	Usually 'confidential'		
Company web site			XXXX
Payroll, retirement values, etc.	XXXX (by employee contract)		
Press releases			XXXX
Brochures			XXXX

<Update this list with your own asset list, and include it in your documentation.>

27 Glossary

Availability – one of the basic dimensions of information security (the others are confidentiality, integrity, and sometimes provability). Availability refers to having the information ready for use when it is needed. Failures in availability include such events as denial of service attacks.

Audit log – same as audit trail. A record in chronological order which is created and retained in order to provide evidence of usage, transactions, intrusion, and other events.

Confidentiality – one of the base dimensions of information security (the others are availability and integrity, plus sometimes provability). Confidentiality is the requirement to protect information from being viewed by unauthorized users. Note that this is not the same thing as *privacy*, a term which means that a person's information is being used in the way the person expected. (See *privacy* in this glossary.)

Custodian is a role relating to the controls over information assets. The custodian does not make decisions about the use of the information, nor grant access – those functions are reserved for the information owner. The custodian does keep controls over the information in accordance with the requirements set out by the information owner, plus with company policies and applicable laws. A typical custodian function would be a database application administrator.

Guideline – a guideline is a lower-level handbook, giving the normal configuration of a system, application, or other tool. The guideline is a recommended method of implementing protection controls for that tool, but need not be followed exactly so long as the protections mandated by *policies* and *standards* are maintained.

Integrity – one of the basic dimensions of information security (the others are confidentiality and availability, and sometimes provability.) Integrity is the ability to ensure that the information is correct at all stages in its life, is safe from unauthorized modification, and hence can be trusted and used.

Owner – a role relating to the controls over information assets. The information owner is responsible for making decisions regarding the protections required for an information asset, plus for granting access, use, copying, and disposal of that asset. This is typically done by a business manager, not done by the *custodian* of the information, by the administrator of a system or application, or by Information Security.

Policy – this word is often used to mean several different things, but the industry is settling in on a single definition for this word. It means a high-level position statement on business direction, and typically includes such items as a privacy policy, one for acceptable usage of company systems, and similar items. It is a document which can be shown to customers, trading partners, investors, and used in public relations.

> This word does not properly refer to the configuration rules at the detailed level, for a given platform, but is still used in that way by some firms. (For example, a 'firewall policy' is really a configuration rule for the firewall – the rule would arise from the corporate policy regarding the security of information, and then from the company

security standards defining which types of access are permissible and what controls are mandated – all of which are defined independent of the actual firewall device finally used to implement the policy and standard.)

Privacy refers to the matching of a person's expectations for the use of their personal information as against the actual use of that information. This usually consists of giving a person proper notice of how the information is to be used, access to seeing how it actually was used, and recourse methods if something goes wrong. Personal information means information which is personally-identifiable, including dates of birth, social security numbers, health care and financial information. Consider a scenario – you receive a telephone call at home, from someone who says that they got your name and number from a local merchant. If that wasn't what you expected the merchant to do, you have a privacy violation according to this definition.

Provability goes by various names, including auditability. It refers to the ability to prove that your controls are proper, so as to minimize legal, regulatory, market or customer dissatisfaction. Consider a situation in which you have every possible control running properly, but you do not have documentation or audit logs – you would not be able to prove your controls, and you might still be liable to regulatory fines or lose in a lawsuit, even if you have experienced no actual losses.

Standard – a standard is the middle-level document, in between *policies* and *guidelines*. Standards give the minimum, baseline protection requirements across platforms, networks, business units, and processes, whereas a guideline gives the recommended, default method of implementing policies and standards onto a given platform.

Threat – a threat is any event, real or possible, which might cause harm to the company or its information. Threats can be protected against, but will still exist. Contrast this with *vulnerability*.

Vulnerability – a vulnerability is a weakness in company systems, procedures, or networks which might permit a threat to actually cause harm. Unlink a *threat*, once a vulnerability is corrected, it goes away, while the threat is still out there, waiting to find a new vulnerability to attack.