For both types of data, it means destroying it in such a way that it can't be recovered. Data destruction policies are influenced by federal and state laws.

These policies help organizations cope with the large amounts of data that they use and produce. Without these policies, records management can be difficult. An organization might not know what types of data it has. It might not be able to find data when it needs it for business reasons. It might use too many resources to store data for longer than it must. Storage space for both paper and electronic data is a valuable resource.

Even if an organization has information security controls in place, data is still a vulnerability. It's vulnerable to external threats such as natural disaster or hackers. It's also vulnerable to unintentional acts committed by employees. For instance, employees can easily delete e-mails that they should keep. They also can save e-mail that should have been deleted because there was no business reason to retain it.

In order to create data retention and destruction policies for electronic data, an organization must know how its IT resources work. They also must know how to retrieve data from these systems. Finally, they must know how to remove data from these systems.

Employee awareness is critical for successful data retention and destruction policies. Employees need to be well educated on data retention requirements. They also need to know how to properly file and maintain data that the organization must retain. Finally, they need to understand proper destruction methods. This is very important to avoid accidental disclosures of either paper-based or electronic media.

Data Retention Policies

Data retention policies define the types of data that an organization has. They also address where data is stored and how it's protected. They specify how long different types of data must be retained. These policies also are called document retention policies.

> **NOTE**
>
> State laws might require governmental agencies to retain financial or other types of data for different lengths of time. This is to meet state auditing requirements or comply with open records laws.

Different types of data have different retention periods. This period is usually driven by a combination of federal and state laws. It's also influenced by business needs. Externally, many federal and state laws govern what organizations can do with their data. These laws also state how long certain types of data must be kept. For example, organizations that are subject to the Health Insurance Portability and Accountability Act (HIPAA) have to retain certain types of data for six years.[11]

Laws aren't the only factor affecting data retention. Organizations also have to think about data retention if they become involved in a lawsuit. Most federal and state courts have procedural rules that require organizations to maintain data if they're party to a lawsuit. This rule might apply even before an actual lawsuit. For example, an organization must retain paper and electronic data in situations where litigation against it is reasonably anticipated. If an organization doesn't maintain this data, it can be sanctioned by a court. Maintaining electronic data for this purpose can be very difficult. There are special rules to follow to maintain electronic evidence that might be used in a lawsuit. They're called E-discovery rules.

In addition to legal requirements, organizations keep data for business purposes. They keep it to conduct business, market products, or to recover from a disaster. Organizations also preserve some types of data indefinitely. This might be because it has legal, fiscal, research, or historical value.

Data retention policies help an organization manage these competing concerns. A cross-functional team helps review and determine data retention requirements. This team should include experts who understand the legal requirements. Expects who know how the organization creates data should be on the team as well. The team must include experts who know the organization's IT systems. This team must understand how the organization uses data and threats to that data.

Data retention policies need to include the following elements:

- Types of organizational data
- Where that data is stored
- How that data is protected
- Legal, business, or other reason for keeping that data
- How long the data should be retained

A data retention policy must be matched with a data destruction policy. An organization must destroy data that it no longer must keep for business, archival, or historical purposes.

Data Destruction Policies

An organization creates data destruction policies to make sure that it destroys data properly. An organization's data destruction process must work hand-in-hand with a data retention policy. The data destruction policy must include the following:

- Identify data ready for destruction.
- Specify proper destruction methods for different kinds of data or storage media.
- Provide validation procedures to make sure data is properly destroyed.
- Provide consequences for improper destruction.

Legal requirements can influence an organization's data destruction policy. For example, the Gramm-Leach-Bliley Act (GLBA) requires that paper documents holding customer information be destroyed.[12] It states that data must be destroyed in such a way that it can't be read or reconstructed. The law also requires that electronic data be destroyed or completely erased. State laws also may require organizations to destroy data in a certain way.

Data destruction policies must be consistently followed. This is important for normal maintenance reasons. It's easy to destroy data when it's done on a regular basis. Following a consistent process is critical if an organization is involved in a lawsuit. It helps protect an organization from claims that it intentionally destroyed evidence.

State Law Data Destruction Requirements

Some state laws require specific data destruction methods. The State of Indiana has this type of law. All business in the state must follow the law. It requires that they properly dispose of the unredacted personal information of their customers. This information includes a customer's Social Security number or certain types of financial account information. The law applies to both paper and electronic information.

The law requires that information be disposed of in a way that makes it unreadable or unusable. It says that proper disposal methods include shredding, incinerating, mutilating, and erasing.

The state can fine a business that doesn't comply with the law. The state may impose fines that range from $500 to $10,000 per violation.

You can read Indiana's data disposal law at *http://iga.in.gov/legislative/laws/2014/ic/titles/024/articles/004/chapters/014/*.

Intellectual Property Policies

Intellectual property laws protect people's or organizations' ownership rights in their creative ideas. It gives them the right to protect their ideas. It gives them the right to profit from their ideas. These rights are exclusive to the owners of intellectual property. They can take action against people who violate these rights.

Intellectual property policies are very important for most organizations. There are two main reasons why an organization should consider an intellectual property policy. They are:

- To protect its own intellectual property
- To make sure that its employees respect the intellectual property rights of others

Organizations have large amounts of data that they use in carrying out their business. This may include information protected by patents, copyrights, and trademarks. It also can include information protected as a trade secret. It's important to the viability of the organization. An organization must protect it.

An organization uses a policy to specify the intellectual property that it owns. As in an AUP, so in a policy governing the use of its intellectual property, an organization will want to state its expectations:

- That the organization's intellectual property may be used only for authorized business purposes
- That the organization's intellectual property may not be disclosed outside the organization
- Whether the intellectual property may be removed from the building, copied onto removable media, or stored in cloud computing infrastructure
- What the rules are for using the organization's name or trademarks in correspondence

There's an information security component to protecting the organization's intellectual property. For example, an organization's electronic proprietary and trade secret data must be secured against internal misuse. It also must be secured against external attack.

The second reason for an intellectual property policy is to make sure that an organization doesn't violate the rights of others. An organization can be held liable for the infringing activities of its employees. For example, an organization will want to make sure that its employees honor software licensing agreements. It will want to make sure that employees don't use software without a valid license to do so. It also must make sure that employees don't copy or distribute unauthorized copies of software. The organization also will want to make sure that employees don't share or download pirated software onto organizational computers.

Authentication and Password Policies

Authentication controls among the most basic types of information security controls that an organization can use to protect its IT resources. **Authentication** is the process whereby a user proves his or her identity to access an IT resource. Good authentication provides controlled access to an organization's IT resources.

The user does this by presenting credentials. **User credentials** are used to access IT resources. They usually include a user name and one of the following:

- **Something a user knows**—This includes passwords, passphrases, and personal identification numbers (PINs).
- **Something a user has**—This includes tokens, smart cards, and digital certificates.
- **Something a user is**—This includes biometric data such as a fingerprint or retina scan.

Organizations can implement authentication methods in many ways. Some ways are more complicated and expensive than others. For example, biometric authentication can be very expensive. Organizations also can choose to implement **two-factor authentication**. This type of authentication requires employees to use two different types of credentials to access IT resources.

Many organizations choose to implement passwords. This is because they can easily implement them. They also are relatively inexpensive to use. Employees generally are familiar with using passwords. Employees may be unfamiliar with other types of authentication methods, such as using biometric data.

There are a number of problems with using passwords as the only authentication method. An organization's IT resources are vulnerable if a password is compromised. A password can be compromised if an employee shares their password. It also can be compromised through a phishing or dictionary attack.

Organizations implement authentication and password policies in an attempt to reduce risk caused by password use. These policies state the user credential rules that employees must follow. Some policies state that an organization's IT department will never ask employees to share their passwords. These policies often include password creation rules. For example, they may state the number of characters that a password must have.

> **NOTE**
>
> A dictionary attack tries to crack passwords by running through words or phrases listed in a dictionary. Strong passwords help combat dictionary attacks.

Would You Share Your Password for Chocolate?

In 2004, a survey at a trade show in London found that more than 70 percent of the people surveyed would reveal their computer passwords to a stranger for a bar of chocolate.[13] The survey was repeated in 2007. In 2007, 64 percent of the people polled were willing to give up their passwords for chocolate. In 2008, only 21 percent of the people surveyed were willing to share their passwords.[14]

The study didn't verify whether people were sharing valid passwords. It's possible that the survey results could be influenced by chocolate lovers sharing fake passwords.

Other common password policy statements include:

- Passwords should not be written down. If they must be written down, that paper should be stored in a secured place.
- Passwords must never be shared with anyone, including trusted colleagues, friends, or family members.
- Passwords must not contain dictionary words.
- Passwords must not include a user's name or parts of their name.
- Employees must create strong passwords that meet character and complexity requirements.
- Passwords expire after a certain period and must be changed.
- New passwords must be different from the previous password or parts of the previous password.
- Passwords may not be reused for a specified period.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.

Information security departments also can create their own policies for how passwords should be used within IT resources. For instance, they might specify that passwords should never be stored in IT resources as clear text. These policies might require that system authentication take place via encrypted channels. These also might specify that passwords can't be displayed on screens as cleartext when an employee enters it. This would help prevent shoulder surfing attacks. Where possible, passwords should expire automatically, and employees should be prompted to create new ones.

Security Awareness and Training

A recent survey asked about corporate information security policies. Two thousand people in 10 different countries took part in the survey. Seventy-five percent of the companies surveyed had information security policies. Forty percent of the employees in those companies didn't know about them.[15]

An important part of any information security program is the training and awareness component. This is because employees play a large role in meeting information security goals. Employees often view information security training as a waste of time. As one author writes, "Given a choice between dancing pigs and security, users will pick dancing pigs every time."[16]

Employee behavior can help protect data and IT resources. It also can be harmful. Employees who aren't aware of their responsibilities pose a threat. They may engage in risky online activities. These activities could harm the organization's IT resources. Their actions also could disclose data. They can subject an organization to liability. Training and awareness activities help reduce this threat.

A high-level policy lets employees know that the BOD supports training activities. An information security awareness and training policy should include the following elements:

- Why security awareness and training is important
- Who has overall responsibility for the policy
- Who provides training and awareness activities
- Which employees must take part in training activities
- How often training must take place
- What the consequences are for not participating in required training

BOD support of training activities is vital. It makes sure that employees understand that training is important. It makes employees take it seriously.

A variety of training and awareness events are necessary to reach employees. Organizations can use multiple training tools to help their employees know about security policies.

Creating an Information Security Awareness Program

Many organizations struggle with information security training and awareness. This includes the U.S. federal government. FISMA requires federal agencies to implement security awareness training. It must be part of their overall information security programs.

The National Institute of Standards and Technology (NIST) created guidance for training and awareness activities. NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program," was published in 2003. It steps organizations through how to design and implement a training and awareness program. It also discusses how to develop training material. Finally, it provides advice on how to review the program's effectiveness.

Any organization can use the NIST guidance to help create an information security awareness program.

Case Studies and Examples

The following case studies and examples show how the concepts discussed in this chapter are used. These case studies are real-world examples of information security governance issues.

Acceptable Use Case Study

> **NOTE**
> You can learn about the company at *http://www.autoliv.com.*

Autoliv is a seatbelt and airbag technology company. In 1998, Autoliv's employee handbook included a number of policies. It stated employee rules of conduct. It included an anti-harassment policy. It also included a computer AUP. Autoliv gave this handbook to all of its employees.

Autoliv's general rules of conduct stated:

- "Each employee is required to be familiar with these rules and with additional rules which apply to particular jobs and operations. In addition, each employee is expected to maintain conduct consistent with job efficiency and accepted standards of behavior for a business environment. Deviation from those standards may be cause for disciplinary action."
- "Disciplinary action may be taken for violation of any single rule or combination of rules, or for other improper conduct or unsatisfactory performance, and may include any of the following actions: 1) Employee discussion; 2) Notice of Caution; 3) Involuntary Suspension; 4) Termination."

Autoliv's anti-harassment policy stated that the company didn't "tolerate or permit illegal harassment or retaliation of any nature within our workforce." Its computer AUP prohibited non-business uses of company e-mail. It also prohibited "conduct that reflects unfavorably on the corporation." [17]

In 1998, Autoliv investigated employee use of its e-mail system. It investigated because of system performance issues. It found that e-mail use was causing the performance issues. It determined that the bulk of e-mail use was not business related.

In June, Autoliv sent an e-mail to all of its employees. It reminded employees about company policy. It said: "E-mail is to be used for business only. We do not wish to 'police' the e-mail system, so your cooperation would be appreciated. Please refrain from sending/receiving these types of messages as it is interfering with legitimate business e-mail."

Autoliv sent another reminder email to its employees in September 1998. This e-mail warned that an employee could be fired for AUP violations.

In January 1999, Autoliv sent another e-mail to its employees. This e-mail stated that it was a violation of the AUP to share chain letters, jokes and stories, and non-business-related announcements. It also instructed employees to delete those types of e-mails and not forward them.

A former employee complained to Autoliv that she had received harassing e-mails from two current employees. Autoliv investigated. It learned that one employee had sent

11 non-business e-mail messages. These messages included jokes, photos, and short videos that were sexually explicit. It found that another employee had sent 25 non-business e-mail messages with similar content. Autoliv immediately fired both employees.

The fired employees filed for unemployment benefits. Autoliv contested this request. A state can deny unemployment benefits if an employee is fired for "just cause." Just cause means that there's a legally sufficient reason for firing an employee. Autoliv said that it had just cause for firing the two employees.

At the unemployment hearing, the employees admitted that they had received Autoliv's handbook. They also stated that they knew about the anti-harassment policy. They said they probably had received the three e-mails about e-mail abuse. They claimed they deleted these e-mails without reading them. They argued that their firing was not "just" because they didn't know they could be fired for sending non-business e-mails.

The Utah Department of Workforce Services found that Autoliv didn't have just cause to fire the employees. This was because the employees said they didn't know that they could be fired for their behavior. They were awarded benefits. Autoliv appealed the agency's decision to the Workforce Appeals Board. It lost its appeal.

Autoliv appealed the decision to the Utah Court of Appeals. Autoliv argued again that the employees had plenty of knowledge that they could be fired for their actions.

Think about the following:

- What do you think the Utah Court of Appeals decided?
- What facts support Autoliv's argument that the employees had knowledge that their conduct was unacceptable?
- What facts support the employees' argument that they didn't have knowledge that their conduct was unacceptable?
- Do you think sending offensive e-mails is a "flagrant violation of a universal standard of behavior"?
- Could Autoliv make any changes to its general rules of conduct, anti-harassment policy, or computer AUP that would make employee e-mail responsibilities clear?

The Utah Court of Appeals reversed the decision of the Workforce Appeals Board. It held that Autoliv did have just cause to fire the employees. In its opinion the court stated: "There are two ways to establish that a claimant had knowledge: 1) the employer must have provided a clear explanation of the expected behavior or a written policy regarding the same; or 2) the conduct involved is a flagrant violation of a universal standard of behavior."[18]

The court held that the employees' e-mail activities had violated a universal standard of behavior. It wrote, "We conclude that in today's workplace, the e-mail transmission of sexually explicit and offensive jokes, pictures, and videos constitutes a flagrant violation of a universal standard of behavior."[19]

You can read the court's opinion at *http://caselaw.findlaw.com/ut-court-of-appeals/1369016.html*.

FYI

The Business Software Alliance (BSA) investigates software piracy allegations for its members. It also files IP theft lawsuits on their behalf. You can read about BSA's anti-piracy program at *http://www.bsa.org/anti-piracy*.

Intellectual Property Example

The Business Software Alliance (BSA) is a trade organization. It represents software companies. Its members include Apple, Microsoft, and Symantec. As part of its activities, BSA runs an anti-piracy program. Software piracy is copying software without permission. It's also sharing copyrighted software without permission. Software piracy is copyright infringement. It's illegal. BSA investigated more than 15,000 cases of software piracy in 2012.[20]

In 1997, BSA received a tip on its anti-piracy hotline. The tip alleged that Oriental Trading Company used unlicensed copies of software on its computers. BSA contacted the company. Oriental Trading Company then conducted an audit of its IT systems. It confirmed that there was unlicensed software on some of its systems.

Oriental Trading Company paid $525,000 to BSA to settle software piracy claims. It also agreed to delete the pirated software from its systems. It agreed to purchase legitimate replacement software. Finally, it promised to strengthen its software management policies.

The BSA has settled similar claims with other businesses. Many of the settlement agreements include terms that require the infringing companies to strengthen their IP policies. How should organizations combat software piracy? What responsibilities do employees have?