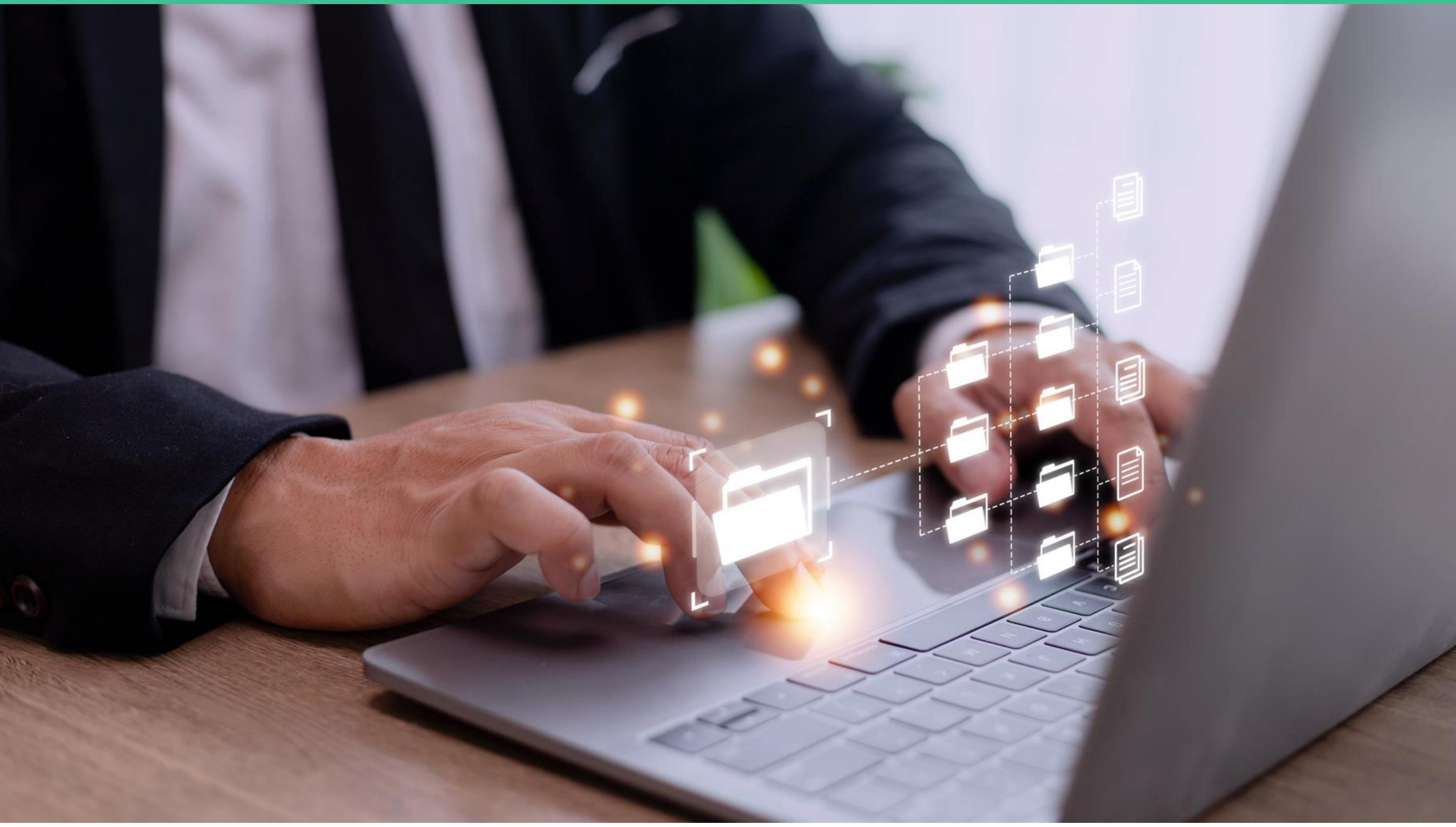
Complior

Secure Storage

eBook

Secure storage is critical to protecting sensitive information and preventing unauthorized access. This e-book highlights the importance of classifying data and storing it securely, as well as how to meet regulatory requirements and mitigate security risks. Regardless of the business, secure storage is an important part of the cyber security strategy for safe and efficient information management.



Complior AB 2024

www.complior.se

Index

What is secure storage?

Secure storage is an important strategy for security-conscious municipalities and companies. By classifying data and information according to sensitivity, you can effectively separate Open information from Security-classified information. This strategy means that classified information is stored separately from the open, within a structure known as secure storage. This protects sensitive information and minimizes the risk of unauthorized access.

The need for secure storage is great, as companies and the public sector store both sensitive and security-classified information. Secure storage is also based a lot on the level of ambition you have and any legal requirements and other regulatory requirements.

What is the purpose of secure storage, and what information do you want to restrict from whom?

The purpose of secure storage is to protect sensitive information and ensure that only authorized persons have access to it. By separating classified information from open data, the risk of data breaches, information leaks and other security incidents is minimized.

Purposes of secure storage:

1. **Protection of sensitive information:** Secure storage prevents unauthorized access to data that may contain personal information, financial information or company secrets.

2. **Compliance:** Many industries have strict regulations and laws governing how sensitive information should be handled, and secure storage helps organizations comply with these requirements.

3. **Risk management:** By storing information securely, companies and municipalities can reduce the risk of a data breach and its potential consequences.

What information do you want to restrict and from whom?

Personal data

Information relating to individuals, such as names, addresses and social security numbers, should be restricted to protect the privacy of individuals.

Trade secrets

Company strategies, customer lists, research results and other business-critical data need to be protected from unauthorized persons, especially from competitors or external threat actors who can use the information to harm the business.

Financial information

Financial reports, payment details and transaction history are sensitive data that must be protected to prevent fraud, theft or misuse. Unauthorized access to this type of information can lead to extensive financial damage.

Critical infrastructure

Information relating to IT infrastructure, energy supply, transport and similar areas are often targets of espionage or cyber-attacks. Protecting these systems is critical to avoiding disruptions to community functions and preventing potential disasters caused by intrusions.

Common security principles

Although organizations' secure storage needs vary, there are several common security principles that should be part of every strategy. These principles help ensure that information is handled and stored securely, regardless of where or how it is stored.

1 Classification of information

Classifying information based on its sensitivity is a fundamental step in applying the right security strategies. By classifying information into categories such as "public", "internal", "confidential" or "critical", organizations can ensure that the right security measures are applied depending on the sensitivity of the data. Classification also helps determine which access controls should be applied and how the information may be shared both inside and outside the organization.

Classification with safety labels

To facilitate the handling of classified information, security labels can be used. A security label is a label assigned to data based on its classification. These labels make the data's sensitivity visible to users and systems, making it easier to follow guidelines for how the information should be handled. Security labels can be applied manually by users or administrators, but also automated based on predefined rules and patterns.

For example, a document containing personal data can automatically be labelled "confidential", which restricts access and enables additional security measures, such as encryption and access logging. By using security labels, organizations can ensure that data is handled correctly throughout its lifecycle – from creation to archiving or deletion.

Automatic classification

To simplify and streamline the classification process, there are today advanced tools that can automate the classification of data. These systems can scan the contents of documents, emails and files to identify sensitive information based on content, metadata or patterns. For example, the system can recognize social security numbers, credit card numbers or other sensitive keywords, and automatically assign an appropriate security label.

Automatic classification reduces the risk of human error, where important information can potentially be forgotten or misclassified. It also ensures that large amounts of data can be managed consistently and with minimal administrative effort.

Watermarking

To further protect sensitive information, watermarking can be used in addition to classification and security labels. Watermarks can be applied to documents to visibly indicate their level of sensitivity, making it more difficult to accidentally share or misuse the information. For example, watermarks can include labels such as "Confidential" or "For internal use only" directly on the document's content, both in digital and printed form.

Watermarks also act as a deterrent to unauthorized persons attempting to distribute sensitive documents, as they make it clear that the material is traceable and marked as sensitive. In some cases, watermarks can also contain information about the document's owner or creator, allowing any data leaks to be traced back to the source.

2 Strong access controls

Access controls are one of the cornerstones of secure storage and a critical component in ensuring that only authorized people have access to the right information. By applying granular and flexible access controls, organizations can define exactly who has access to which data, under what circumstances and with what rights. This helps reduce the risk of unauthorized access and protects sensitive information from falling into the wrong hands.

Role-Based Access (RBAC) and Attribute-Based Access (ABAC)

Traditionally, role-based access control (RBAC) has been a common method of managing access within organizations. This model assigns access based on the user's role within the organization. For example, a user with the "administrator" role may have broader rights than a "user," and these roles control what information can be viewed, edited, or shared. RBAC is relatively easy to implement and understand but can be limited in situations where more flexible and dynamic access decisions are required.

Attribute-based access control (ABAC) offers a more sophisticated and flexible approach to managing access. Rather than basing access solely on a user's role, ABAC considers multiple attributes (properties) that may include the user's identity, time, location, device type, data sensitivity level, and other contextual factors. This allows organizations to create more dynamic access controls that can be adapted to specific situations and risk levels.

Granular access controls with ABAC

With ABAC, access controls can be specified at a very detailed level. Some of the key factors that can be used in attribute-based access control include:

Who can access:

Access is based not only on the user's role, but also on their individual attributes such as their security credentials, employment status, or their relationship to the data they are trying to access.

When and from where access can take place:

Through ABAC, access decisions can depend on contextual attributes such as time and location. For example, a user may have access to certain information only during office hours or only from the company's network. If the user attempts to access the data outside of these conditions, access may be denied.

What type of access is granted:

ABAC enables fine-tuned control of what a user can do with the information. This may include rights such as read only the data, edit it or share it further. For example, a user can be given access to read but not edit a document or be given the ability to edit a file but not share it outside the organization.

Advantages of ABAC in Safe storage

Dynamic and flexible access management:

By using multiple attributes and combining them, organizations can implement more advanced access rules. This is particularly useful in complex environments where users need access to different types of information depending on the context.

Enhanced Security:

By including factors such as location and time, ABAC can ensure that access is only granted under secure and controlled conditions, reducing the risk of unauthorized access in the event of, for example, network intrusion or stolen login credentials.

Better compliance:

With ABAC, organizations can ensure that their access policies comply with specific laws and regulatory requirements, by specifying and automating access rules based on the requirements placed on different types of information.

Examples of using ABAC

An employee may be able to access an internal report when they are on the company network during work hours but be denied access when they try to log in from a personal device outside of work hours.

Sensitive data, such as trade secrets or personal data, can be automatically protected depending on the device being used, ensuring that only devices that meet security requirements have full access.

3 Secure information sharing

Secure information sharing and collaboration

Being able to share information securely is a critical function for many organizations, especially those working on projects with external partners, suppliers or consultants. Ensuring that sensitive information does not fall into the wrong hands requires robust tools and methods that allow files and documents to be shared securely, while access is closely controlled.

Encrypted information sharing

Encrypted communication channels are used to protect data during transmission and storage. By using tools that enable encrypted sharing of files and documents, organizations can ensure that only authorized recipients have access to the information. Encryption makes it impossible for unauthorized persons to read the content, even if it were intercepted or stolen in transit.

Granular access when sharing information

It is important to be able to share information with the right people and with the right permissions. An effective information sharing tool makes it possible to:

- **Set different access levels**, such as "read only", "edit" or "share".
- **Revoke access if needed,** for example if the recipient no longer needs access or if security requirements change. This gives the organization full control over the shared information throughout the sharing process

Secure reader for read-only access

A common solution to prevent unauthorized dissemination or misuse of shared information is to use a **secure reader**. This means that the recipient can only read the information via a secure viewing application that prevents:

- **Copying of text and content.**
- **Downloading the document to a personal device.**
- **Screenshot or other means of extracting information.**

This method ensures that the information can be shared in a controlled manner and minimizes the risk of sensitive data being disseminated, even if the document has been shared with external parties.

Prevention of proliferation and abuse

One of the biggest challenges with information sharing is preventing shared information from spreading further without control. There are several techniques and tools that can be used to minimize these risks:

- **Block email attachments:** Shared information can be configured so that it cannot be attached to emails or uploaded to external storage areas such as cloud services. In this way, the organization can ensure that sensitive data remains within controlled channels and is not disseminated uncontrolled.

- **Traceability and audit logging**: All shared information should be traceable. This means that the organization can see who has opened, edited or shared the document, as well as when and where this happened. Traceability provides an extra level of accountability and security, deterring unauthorized use of shared information.

Watermarking for increased security

Using **watermarking** is an effective way to further protect shared information. By applying automatic watermarks to documents, indicating that the material is confidential or belongs to a specific department, organizations can clearly demonstrate that the information is protected. Watermarks can also include the recipient's name or email address, which creates a deterrent effect and makes it possible to trace any leaks.

Usage policies based on recipients

Another important aspect of secure information sharing is applying **individual policies** depending on the recipient and their role in the organization or project. For example:

- **External consultants** may be allowed to open a document, but a policy may force it to be opened in "read-only" mode and with a visible watermark indicating that the document is confidential. This watermark may also include the recipient's name or email address to discourage unauthorized distribution.

- **Project employees or internal team members** can be given full editing access to the documents. This may include the ability to open and process files in regular programs, such as Microsoft Word, to facilitate daily work with the project material.

Having **granular usage policies** based on the recipient's relationship to the organization ensures that each individual gets exactly the level of access required for their data, and nothing more.

Customized security levels depending on the type of document

Different types of information, such as blueprints, financial reports or project documents, require different levels of security depending on their sensitivity and who they are shared with. Organizations should be able to set specific security policies for different types of information

- **Drawings** can, for example, be shared with external construction contractors with the option to only read and comment without downloading the document.

- **Reports** can be shared with financial partners with access to both read and edit capabilities, depending on their role in the project.

4 Prevent data theft and dissemination

Strong security measures to protect information:

To protect information from being stolen or disseminated, knowingly or unknowingly, it is crucial to implement strong security measures. These security measures help organizations deal with both internal and external threats and ensure that sensitive information remains protected.

Here are some of the key actions:

Data encryption both at rest (stored) and in transit:

Encryption is a basic security method to protect data from unauthorized access. Encrypting information both when it is stored and when it is transferred between systems ensures that even if the data is intercepted, it cannot be deciphered without the correct encryption key.

Data Loss Prevention (DLP):

DLP systems are used to identify and block unauthorized transfers of sensitive information, such as personal data or company secrets. These systems monitor and analyse data flows, both internal and external, and can automatically take actions such as blocking or alerting when sensitive data attempts to leave the organization's network in an unauthorized manner.

Automatic discovery of sensitive data:

Modern security systems can automatically scan and identify sensitive information in the organization's network, documents and e-mail. This automatic detection ensures that even undetected or unclassified sensitive data can be located and protected. For example, the system can detect personal data, financial data or intellectual property rights, and ensure that this data is handled in accordance with the company's policies and regulations such as GDPR.

Automatic labelling of sensitive data:

When sensitive data is identified, automatic labelling systems can apply security labels based on the content or context of the data. This means that all sensitive information is automatically given the correct label, such as "confidential" or "for internal use only", without the user having to intervene manually. Automatic tagging helps ensure that security measures are applied consistently and that the right level of protection is applied to all sensitive data

User training:

Even the best technological solutions cannot completely eliminate the human factor. User training is an important part of security work. By training employees to understand the importance of protecting sensitive information and how to avoid common security risks, such as phishing or insecure handling of data, organizations can reduce the risk of accidental security incidents. It is particularly important that users learn to identify warnings from security systems and follow internal procedures for information management.

5 Traceability and logging

Clear traceability through logging of all access attempts and data transactions is a critical component in being able to detect, investigate and prevent security incidents. Logging acts as a "black box" for the system, providing visibility into how data is managed and used. By monitoring and documenting every interaction with sensitive information, an invaluable tool is created for both proactive and reactive security management.

What should the logging include?

Effective logging should cover several aspects of data access and use to ensure full traceability:

Who Accessed: Identification of the user (including their role or permissions) attempting to access information. This includes both internal users and external parties, such as consultants or suppliers. The log must also be able to be linked to the individual's authentication method (e.g. password, two-factor authentication).

When Accessed: Exact timestamps for each access attempt or data transaction. By knowing when a specific action occurred, the organization can quickly identify suspicious or unauthorized access attempts during irregular hours, such as outside regular business hours.

From where the access was made: Information about the location or device where the access took place, such as IP address, network location or the device used (eg mobile, computer or tablet). This makes it possible to trace whether the access was made from secure networks or from potentially unsafe or unauthorized locations.

What the user has done with the data: It is not only important to know that someone has gained access to the data, but also what they have done with it. Logging should include which files or data have been accessed, modified, shared, copied or deleted. This provides a complete picture of user activity and can help identify potentially malicious behaviour, such as copying large amounts of data or sharing sensitive information with unauthorized parties.

Security incidents and investigation

A well-developed logging function enables organizations to quickly and efficiently identify potential security incidents. In the event of a data breach or other security breach, the logs can analyze exactly how the breach took place, what data was exposed and how big the threat was. This enables a rapid and targeted response, including isolating the incident, stopping further intrusions and implementing recovery actions.

Compliance and reporting

In many industries, particularly in the public sector, finance and healthcare, organizations are required to comply with specific laws and regulations that require traceability. Examples of such regulations include the General Data Protection Regulation (GDPR), which requires organizations to be able to demonstrate that personal data is handled securely and that all access attempts to this data are documented. Logs help organizations meet these requirements by providing a history of how data has been handled and by whom.

If an organization suffers a security incident where sensitive information is compromised, it is often required to report to regulatory authorities. Clear and detailed logs enable the organization to quickly compile the necessary information and prove that appropriate measures have been taken to protect data. This can reduce fines and other penalties and improve the trust of customers and business partners.

Automation and analysis

Many modern security systems use automated logging and analysis tools to quickly detect anomalies in user behavior and potential security threats. For example, such systems can warn if a user suddenly starts downloading unusually large amounts of data, or if access attempts are made from an unusual location. Automated incident response can also be used to block access immediately if a potential breach is detected, limiting damage before it escalates.

The role of logging in auditing and security improvement

Logs also play an important role in regular security audits. Organizations can use log data to analyze access patterns, identify weaknesses in access controls, and adapt their security policies over time. By regularly reviewing logs, potential security flaws can be discovered and fixed before they are exploited by unauthorized persons.

6 Encryption

Strong encryption is a fundamental security measure to protect sensitive information, both when it is stored and when it is transmitted. Encrypting data ensures that even if information is stolen or lost, it cannot be read by unauthorized persons.

Encryption should be used on all sensitive data, and organizations should regularly update their encryption methods to stay in line with the latest security standards.

Regardless of whether the encryption takes place on a local file server or in a public cloud service, it is important to meet the requirements for HYOK (Hold Your Own Key). With HYOK, the organization gains complete control over its data by creating, storing and managing the encryption key itself. This key is protected by an HSM (Hardware Security Module), which ensures that the key is stored and handled in a very secure manner.

By using its own encryption key, the organization can protect its data independent of third-party providers, and thus has full ownership and control over the data. This means that the encryption key can be stored in Sweden, under Swedish sovereignty and legislation, which is crucial to ensure compliance with local regulations and protection against foreign jurisdictions.

An important protection that HYOK offers is that it prevents, for example, a cloud provider from being forced to release data under laws such as FISA (Foreign Intelligence Surveillance Act) in the US, because the provider does not have access to the encryption key. Additionally, HYOK prevents the cloud provider's administrators, or a potential attacker who steals their keys, from accessing the organization's data. Keeping control of its own encryption key minimizes the risk of unauthorized access and ensures that no one but the organization itself can decrypt and access the sensitive information.

Complior

Ensuring a robust secure storage solution requires not only technical solutions but also compliance with legal and regulatory requirements. By using modern methods of encryption and key management, companies and organizations can guarantee full control over their data, whether it is stored locally or in a public cloud service.

Complior offers a wide range of security services for organizations that want to protect their most sensitive data. Through its **PCI DSS certified cloud infrastructure** and services such as **HSM** and **Key Management Systems (KMS),** companies can easily implement secure solutions for storage, key management and compliance with regulations such as GDPR and PCI DSS, DORA, NIS2.

Complior offers a complete solution for secure storage through encryption and key management, whether on-premises or in the cloud. Our strong partnership with **archTIS** has expanded our solutions with **NC Protect** and **NC Encrypt**, which enable customers to automatically classify and protect unstructured data in Microsoft 365 and other environments. Through **HYOK (Hold Your Own Key)** and integration with local KMS, customers gain full control over their encryption keys, guaranteeing data sovereignty and protection.

More information about Complior and solutions can be found here : www.complior.se/products

Complior not only offers the tools for secure storage and encryption, but also a trusted partner that ensures organizations can stay in line with international and local laws, while maintaining full control over their most valuable data.

Complior