



SECLORE FILESECURE

Share with Confidence !

Engineering Services

CASE STUDY

Background Of The Organization

Client is a unit within one of the largest Engineering Procurement & Construction & Steel companies in the world with presence in more than 100 countries and revenues of more than Euro 50 Billion.

Process Before

A typical project team would consist of members from customer organization, design & project execution unit, procurement unit and vendors. Frequently, confidential data would be exchanged between team members as unsecured and uncontrolled emails. Such emails would typically contain data controlled by strict non disclosure agreements (NDAs). Project teams exchanging data were not always informed of these NDAs. The confidential documents were created on computers distributed across geography, networks and domains.

Security Risks and Data Leakage

Many approaches to secure documents and files were considered for adoption to ensure that the information exchanges amongst team members were protected against data leakages. Traditional security mechanisms were not suitable since they failed as soon as the document left the enterprise control area via email as there was no method to track or control the usage of these documents.

Whenever a member of a project team left the organization, important documents like designs and project plans were frequently lost. The nature of the projects sometimes warranted appointing vendors to provide specialized services. Such associations required sharing of confidential information for the vendor to process it further . For vendors giving design consulting services, there was no way to ensure that intellectual property of designs was restricted for use within the specific project. In general, once authorized users gained access to the information there was no way of controlling its usage. Because of these factors the client decided to have all vendor personnel delivering services to operate out of the client location. This had a huge implication on the ongoing costs and overheads for project execution.

Need for persistent security and usage control of documents

Encryption, password protection and access control of documents were ruled out as solutions to the problem because of the lack of persistence of security. A thorough analysis by the internal information security team identified the need for an information usage control system that would enable information security without restricting collaboration. The enterprise also identified also the need to implement usage control of document. Some of the key capabilities sought were:

- Capabilities to control editing, printing and distribution rights
- Possibility to control whether the documents can be accessed when the recipient is offline
- Dynamic modification of the usage rights and applying the same even to documents already distributed.
- Full audit trail of access and usage of documents within the enterprise or from outside.
- Granular control of usage rights (view / print / edit / forward) per document
- Possibility to modify usage rights for the documents remotely, without the need to re-send the document.

The Seclore Solution

The Seclore FileSecure Solution for desktops enabled sharing of rights protected documents across the enterprise without the need to manually password-protect them. Documents are protected with a simple desktop utility which can be used within and outside of the enterprise by authenticated users. Full audit trails are available to users for their documents as well as to the central administrator. Granular usage rights for viewing, printing, editing or forwarding documents are configured for online or offline usage of documents. Dynamic rights management allows revocation of rights based on events like resignations and transfers.

Control

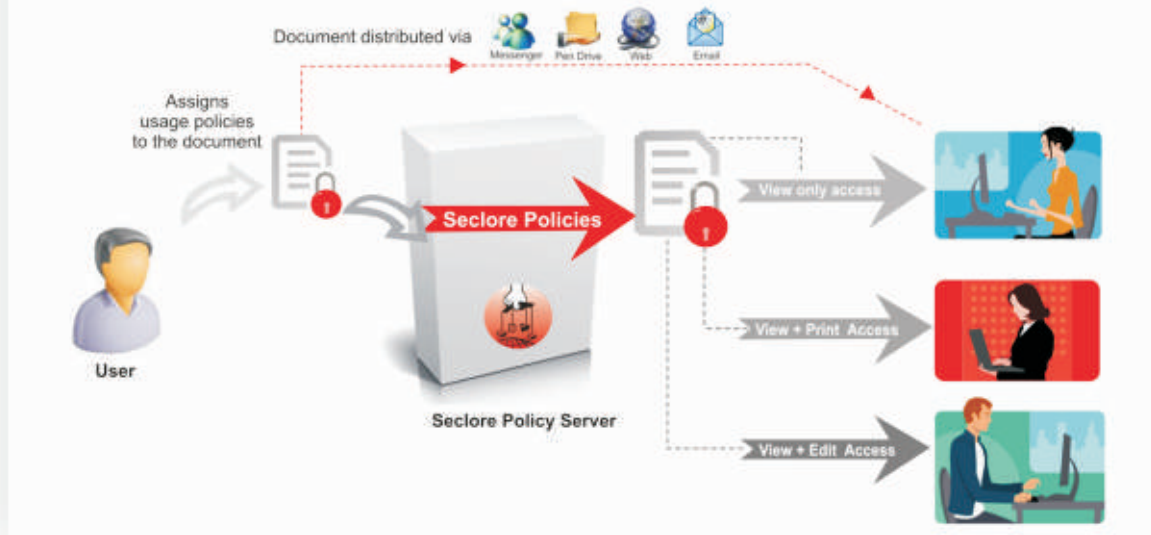
Who: Only specific users belonging to the project team spread across client organization, customers and vendors

What: Viewing, editing, printing, distribution rights specific to each user and group

When: For the period of the project involvement or earlier

Where: From specific locations or not

Seclore FileSecure for Desktops/Laptops



Benefits And ROI Drivers

Seclore file Secure for Desktops provided the client with persistent end-to-end control over its information through the life cycle of creation, storage, transmission, usage and destruction. Documents owners have full control over the usage of their documents, along with complete audit trailing of how they are being used. Dynamic rights management allowed for centralized revocation of rights based on status changes.

About Seclore

Incubated and promoted by IIT Bombay, Seclore Technology develops innovative solutions in the area of information usage control. Seclore has achieved industry leadership in the area of information usage control, information rights management, enterprise DRM through its range of products. Some of the largest corporations in financial services, engineering and education use Seclore products for information usage control.



SECLORE

Tel: +91 22 4015 5252

Email: info@seclore.com

Blog: <http://blog.seclore.com>

www.seclore.com