

**Do you need to monitor the flow and usage of confidential information for compliance to SOX, HIPAA, PCI, etc.**





ISO audits typically focus on information access within applications and folders, while ownership and acceptable use of unstructured information in the form of documents and emails is left out. Malicious intent, errors, omissions & lack of awareness could make this information publicly available leading to legal action, monetary and reputation losses

## SECLORE FILESECURE

Share with Confidence !

Seclore FileSecure enables compliance to key controls within the ISO frameworks like establishing inventory, ownership and acceptable use policy for unstructured information which has been till now very difficult to bring into the ISO fold. By allowing classification, usage audits, incident management and forensics, Seclore FileSecure enables organizations to be compliant to ISO XXXX through the life cycle of the information

Seclore FileSecure allows enterprises to define and implement information usage policies. A policy is an "answer" to four Questions i.e.

🔒 **WHO** can use the information

People & groups within and outside of the organization can be defined as rightful users of the information



🔒 **WHAT** can each person do

Individual actions like reading, editing, printing, distributing, copy-pasting, screen grabbing etc. can be controlled



🔒 **WHEN** can he use it

Information usage can be time based e.g. can only be used by Mr. A till 25th Sept or only for the 2 days



🔒 **WHERE** can he use it from

Information can be linked to locations e.g. only 3rd floor office by private/public IP addresses



Seclore Technology (incubated and promoted by IIT, Bombay) is a leading provider of information security solutions in the areas of information usage control, information rights management (IRM) and secure outsourcing. Its expertise lies in protection of data post distribution irrespective of its location or mode of transfer.



# SECLORE