LEARNING THEORIES 4

RECORDS MANAGEMENT SECURITY

What Is Records Management Security

RECORDS MANAGEMENT REQUIRES APPROPRIATE PROTECTIONS FOR BOTH PAPER AND ELECTRONIC INFORMATION

three main parts to records management security;

1. ensuring protection from physical damage,
2. external data breaches,
3. and internal theft or fraud..

Organizations face a range of security threats that come from all different angles, including:

INTERNAL THREATS

Employee theft and misuse of information

EXTERNAL THREATS

Data breaches caused by viruses, trojans, and other forms of malware

NATURAL DISASTE

Fire, flood, and other natural disasters

Why Using Different Security Types Is Important

HOW TO CONTROL RECORD-LEVEL ACCESS

Organization-wide defaults
specify the default level of access users have to each other's records.

Role hierarchies
ensure managers have access to the same records as their subordinates. Each role in the hierarchy represents a level of data access that a user or group of users needs.

Sharing rules
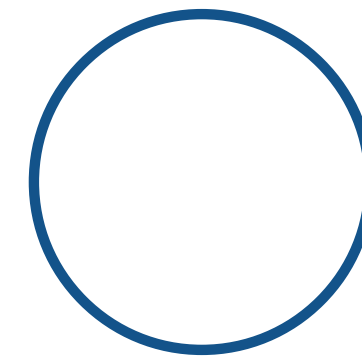are automatic exceptions to org-wide defaults for particular groups of users, to give them access to records they don't own or can't normally see.
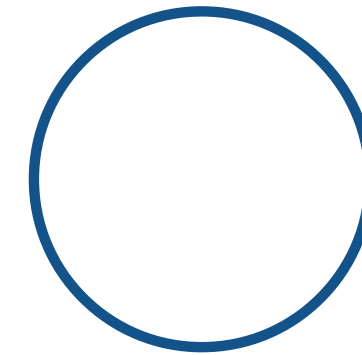
Manual sharing
lets record owners give read and edit permissions to users who might not have access to the record any other way.
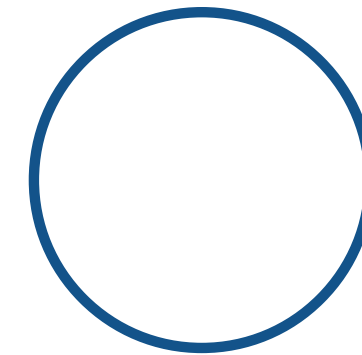
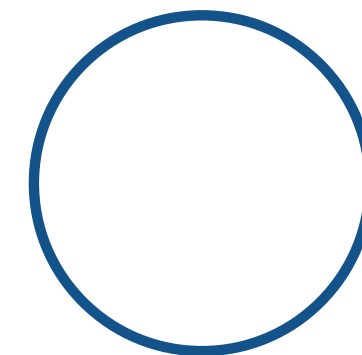**Types of Security Classification & Secured Accessibility**

The Power of Visual Charts

SECRET

CONFIDENTAL

INTERNAL USE

OPEN

Category	Description	Level
Secret	Official records which if wrongly exposed to external parties, could have a significant negative impact to strategies, security, company reputation and business opportunities of the organization. They are generally business strategies, plans, innovations and security arrangements.	Strategic
Confidential	Official records which, if wrongly exposed to external parties, would cause a serious negative impact to the business operations of the organization. They generally relate to business operating records, transactional data and personal matters.	Operational
Internal Use	Official records which, if wrongly exposed to external parties, would cause a negative impact to the business administration of the organization. They are generally accessible to a specifically identified group of staff and require a certain degree of protection from public knowledge.	Administrative
Open	Records which have no business value to external parties and generally cannot be used against organization.	None

TYPES OF SECURITY FOR PAPER RECORDS

Locked Storage Areas
in site records storage

Secure Storage Facilities
off site records storage

Fire and Flood Protection
off site records storage

Document Redaction

documents can be redacted during the scanning process itself to obscure sensitive parts of new digital documents.

File Encryption

document management systems incorporate encryption tools

Access Control Lists

used for limiting access to sensitive files for only those who need it.

TYPES OF SECURITY FOR ELECTRONIC RECORDS

PROTECT YOUR RECORDS!