

Curtain e-locker – Protecting Your Files

Internal Document Security Best Practice

Coworkshop Solutions Limited





Internal Document Security Best Practice

- Know the current security trend
 - Reference web site, for example
 - www.securityfocus.com
 - www.cert.org
- Plan ahead before the security breaches and incidents
- Have a contingency planning and formal report channels ready for security incidents
- Form an security organization
 - Security Manager/Officer
- Enforce the administrative security policy and standard
- Increase security awareness of employees



Internal Document Security Best Practice

- Maintain security and incident log of valuable assets
- Proactively monitor for noticeable data irregularity
- Classify valuable data/assets into different categories and assign user access accordingly
- Perform daily backup for sensitive data and test the backup/restore procedure periodically
- Provide formalized channel for employee to report colleague's problematic behavior
- Disable terminated employee connection to network including closing remote open connection (VPN connection)
- Deny physical access to terminated employee



Internal Document Security Best Practice

- Avoid to use share accounts and passwords for sensitive data
- Enforce to use password-protected screensavers to workstation
- Maintain procedure and technical controls on the system administrators and privileged users



End