BEST PRACTICES IN USER DATA MANAGEMENT

WITH NORTHERN

NORTHERN

CONTENTS

NORTHERN

INTRODUCTION

Northern's User Data Management software solution can be used to achieve a wide variety of goals. This document provides an overview of some of the common working practices that Northern's customers have established. It describes how technology-supported workflows are being used within these organizations to tackle specific risk or efficiency problems.

ABOUT NORTHERN

The vast majority of organizations have little to no understanding of their file data. The data that they are legally responsible for. The data that is the result of thousands of hours of invested effort. The data that forms a key asset and source of competitive advantage. What is valuable to us and what is not? What is valuable to our competitors? Which files contain data subject to external regulations? These are fundamental questions that, incredibly, remain unanswered.

Organizations have been in a state of paralysis. Fixed in the belief that efficiency gains were the only benefits available from pro-active data management, and that these rewards could not warrant the investment necessary.

The situation is changing. Tightening regulatory frameworks, high-profile data loss cases, the adoption of off-premise storage solutions, the advent of process-oriented solutions. There are numerous factors behind the accelerating realization that user data must, and can, be scrutinized.

Northern is supporting some of the world's leading organizations in their identification and improvement of on-going working practices that currently ignore the costs, risks and/or value of the unstructured data involved. The benefits realized by these customers include:

- Increased process and cost efficiencies
- Improved regulatory compliance and risk management
- Rationalized data retention and improved dissemination of business knowledge
- The identification and implementation of innovative working practices

Some examples of how organizations are using Northern's standardized software solution to achieve these goals include: ensuring valuable data is not neglected when users leave the organization, forcing users to delete sensitive reference material after use, enforcing strict rules on the location of specific record types at creation, mapping file service use to internal/external regulations and requiring that data owners self-regulate.

Northern uses a sequential approach where needs are resolved in order of priority and value delivered quickly; identifying and prioritizing on-going business problems and resolving them via minimal adjustments to existing working practices. Solutions are integrated with current tools and data repositories.

IDENTIFY AND REMEDY DANGEROUS WORKING PRACTICES

IMPROVE USER HANDLING OF ORGANIZATIONAL RECORDS	
TARGETTED BEHAVIOUR	Working copies of Records are being abandoned in unsecured locations.
DIRECTIVE	Files temporarily retrieved from records management systems for editing or reference, must be returned correctly to the records management system after edits have been made and all reference copies must be deleted as soon as work is complete. Records may not be indefinitely stored in Home Drives, SharePoint Sites, Office365 file shares, or on NAS storage. Records may only be stored in designated records management systems.
POLICY REQUIREMENTS	• Scan once per week for files containing 'customer numbers', 'employee numbers', 'supplier numbers', social security numbers, credit card numbers, and/or other specific PII/PCI data. That have not been accessed/modified within the past seven days. • Notify Data Stewards/Records Managers when suspected records have been identified. • Require that Data Stewards/Records Managers review file lists and perform appropriate actions.

AVOID UNNECESSARY RETENTION OF SENSITIVE JOB APPLICANT DATA	
TARGETTED BEHAVIOUR	Personal letters and CVs collected during recruitment processes are being retained within Managers' Home Drives. The sensitive personal data within these files is not appropriately secured.
DIRECTIVE	Personal letters and CVs collected during recruitment processes must be destroyed immediately after the position is filled. If the manager wishes to retain these documents for future reference then a dedicated location can be provided.
POLICY REQUIREMENTS	• Home Drives (including O365 file storage) are scanned on a monthly basis. • Files containing relevant strings/patterns (social security number, "CV", etc.) are identified. • The owners of identified files are notified, asked to remove the offending files and reminded of the organizational directive.

NORTHERN

REMOVE PRACTICES OF STORING PASSWORD DETAILS IN FILES	
TARGETTED BEHAVIOUR	Users are storing personal passwords as well as application and service account login information in file shares.
DIRECTIVE	Users must store all login credentials (including user names and passwords for personal accounts) in a dedicated system (KeePass). No ID or password information may be stored in files, encrypted or otherwise.
POLICY REQUIREMENTS	• File shares and O365 file storage are scanned once per month. • Files containing text strings associated with passwords and user IDs are identified. • The owners of identified files are notified, asked to check the file contents and reminded of the organizational directive.

ENSURE DESTRUCTION OF SENSITIVE ANNUAL REVIEW DATA	
TARGETTED BEHAVIOUR	Sensitive personal data, including salary information, is distributed to managers on an annual basis to support annual review processes. These files are not being appropriately deleted after the conclusion of review processes.
DIRECTIVE	Employee information that is provided in support of annual review processes must be deleted following completion of these processes. Historical information can be provided upon request and should therefore not be retained independently by managers.
POLICY REQUIREMENTS	• Home Drives (including O365 file storage) and Common Shares are scanned on a monthly basis. • Files containing relevant strings/patterns (“Annual Review”, “Salary” and employee numbers) are identified. • The owners of identified files are notified, asked to remove the offending files and reminded of the organizational directive.

NORTHERN

EFFICIENCY IMPROVEMENTS IN FILE SERVICE USE

REVIEW OF DATA FOOTPRINT AT EMPLOYEE DEPARTURE/TRANSFER	
TARGETTED BEHAVIOUR	A significant volume of files stored in the file service are owned by ex-employees or are no longer in use because the file owner's role has changed. The data within these files, which carries unknown risk and unknown value, is unused and unmanaged.
DIRECTIVE	It is each employee's responsibility, or the responsibility of their supervisor, to properly manage records prior to transfer or departure. Records must be retained or disposed of in accordance with approved records retention and disposition schedules
POLICY REQUIREMENTS	• A standard analysis of file shares owned or used by the departing/transferring employee are run prior to, or at the time of departure/transfer. • Employees/managers review files listed by these analyses and ensure that data management controls are being properly followed (delete transient files, delete duplicates, delete personal files, customer records correctly located, etc.). • Completion of data review is documented.

CREATE AWARENESS AND ENCOURAGE EFFICIENT FILE SERVICE USE	
TARGETTED BEHAVIOUR	Workplace organization practices are in place for the physical workplace (4S). These must be extended to electronic data spaces.
DIRECTIVE	File storage that is allowed to grow without any form of management will quickly present unnecessary and significant risk and cost. This can be avoided by extending the corporate culture for structure and cleanliness in the physical workspace to include use and content of the file service.
POLICY REQUIREMENTS	• File shares and SharePoint sites are periodically scanned to identify redundant, obsolete and trivial files (ROT). • A user designated as the Data Steward for each department is provided with access to the results of these analyses. • It is the Data Stewards task to identify and take each opportunity to improve how the department is using the file service. • The Data Steward may delegate access to analyses for specific users and request that they assist in removing their ROT data.

NORTHERN

CONTROL DATA GROWTH AND GUIDE DELETION OF TRANSITORY FILES	
TARGETTED BEHAVIOUR	Personal and common file shares are growing at approximately 60% p.a. Much of the content of these storage repositories is redundant, obsolete and/or trivial. Users and teams are hoarding irrelevant data.
DIRECTIVE	Hard or soft limits for file share size should be put in place. These should be used to indicate to the users what the expected suitable size is for a file share. Users should have access to actionable-reports that guide clean-up of file shares when limits are approached/reached.
POLICY REQUIREMENTS	• Hard quotas are configured on users' personal (Home) folders. Notifications are sent to the Home Drive owner when quota thresholds are reached. These emails include a link to self-service dashboards. • Soft quotas are configured on common (Department, Project) shares. Notifications are sent when quota thresholds are reached. These emails are sent to the last ten users who wrote into the share and include a link to self-service dashboards. • File shares are scanned on a weekly basis. The data is used to refresh self-service dashboards that users have continuous access to. These dashboards list files that are likely candidates for clean-up (old, duplicated, non-business-related file type, etc.).

REFINE AND ORGANIZE PROJECT DATA AT PROJECT CLOSE	
TARGETTED BEHAVIOUR	Project teams are not reviewing project data on project completion. Large volumes of data are being retained and archived for long periods when only a small volume of that data is subject to retention policies. As project teams are dispersed after project close, knowledge of what should / should not be retained is quickly lost.
DIRECTIVE	Project working practices should be extended to include a data review step. Project Managers are responsible to ensure that all project data is reviewed and organized at project close; records are identified and all other working documents, copies/versions, reference material, etc. are deleted.
POLICY REQUIREMENTS	• Regular scans of project folders are carried out. These scans populate self-service dashboards designed to highlight files that are suspected to have low importance. • Project Managers should periodically review the content of file shares related to their project(s) – identifying and deleting unused files. • When a project is concluded, Project Managers perform a full review of associated file shares – ensuring that all files subject to retention periods are moved to an appropriate location, other important files are appropriately named and organized, and all other files are deleted.

NORTHERN

DELIVERING ON SPECIFIC AUDIT REQUIREMENTS

TEST TO ENSURE RECORDS ARE CORRECTLY LOCATED	
TARGETTED BEHAVIOUR	Compliance to written policies for record location is not being actively monitored.
DIRECTIVE	Tests must be performed to confirm that users and Data Stewards are correctly locating files containing PII or PCI data according to standards.
POLICY REQUIREMENTS	• Tests must be performed on a weekly basis to ascertain if files suspected to contain PII or PCI data are being stored in SharePoint sites or OneDrive for Business file stores. • Presence of 'customer numbers', 'employee numbers', 'supplier numbers', social security numbers, credit card numbers will signify a failed test. • Results of each test are sent to Records Managers. • Tests will be performed on a monthly schedule and available to Record Managers and Data Security personnel to run on an adhoc basis.

WORKFLOW FOR RESPONDING TO LEGAL HOLD REQUESTS	
TARGETTED BEHAVIOUR	Requests to place data related to specific people, projects, products or cases on Legal Hold are being poorly fulfilled. A lack of sufficient insight into data content is leading to unnecessarily large volumes of data being quarantined and to relevant data being excluded.
DIRECTIVE	A scientific method of identifying files that should be subject to legal hold is required. The organization is exposed to unnecessary (and significant) infrastructure and services costs when excessive data is placed on legal hold. Similarly, the organization is failing to fulfil its legal obligations when relevant files are missed. The ability to query file content and identify the presence of relevant strings is necessary.
POLICY REQUIREMENTS	• Legal announces that all data connected to a person, company, case, etc. should be placed on legal hold. • IT identifies the Data Stewards (Business Unit Managers, Department heads, Records Managers, etc.) that should be involved, and creates the quarantine location with relevant permissions, retention policy, etc. • Data Stewards provide lists of the data repositories that should be scanned (text-mining) for files connected to the person, company, case, etc. Scans are configured and executed. • Data Stewards receive notification when data is collected and review file lists - moving relevant files to quarantine.

INTEGRATING FILE SERVICE DATA INTO OTHER SYSTEMS

ENRICHING INCIDENTS GENERATED BY OTHER SYSTEMS	
TARGETTED BEHAVIOUR	Security staff find it difficult to prioritise data loss, system failure, data breach, etc. incidents as they lack knowledge of the sensitivity of the data that was lost, has become unavailable, or was unlawfully accessed.
DIRECTIVE	Incident alert tickets should include relevant information gathered from other systems. In the case of data loss, system failure and data breach incidents, information should be available that exposes the sensitivity, importance and frequency of use of the data in the affected file shares/systems.
POLICY REQUIREMENTS	• An incident is triggered by another system that concerns a file share, SharePoint site, etc. • The creation of the incident runs a set of standard analyses for that repository; identification of PII/PCI that were accessed/modified at the time of the breach, files that may contain password information, etc. • The incident management system can also connect to results of analyses that were previously collected via a recurring schedule. • Links to related dashboards are added to the incident. • Security staff use the additional information to help prioritise and analyse incidents.