Document Retention Checklist

Does your organization have a formal, written, records retention policy in place? In many industries, organizations are unsure of what they should or shouldn't be keeping and by default, many just keep everything. However, keeping it all is not good records management. If your organization is ever involved in litigation or a regulatory inquiry where you have to produce information, you need to be able to quickly and securely access your data. Making a plan is easy, just start by following our simple five step outline below. Can you answer these questions?

MAKE A PLAN

- ☐ Where is your data?
  - ☐ Paper Documents / Filing Cabinets
  - ☐ Electronic Documents / Computers / Mobile Devices Flash Drives / Disks
  - ☐ Emails
  - ☐ Websites
  - ☐ Digital Copiers / Printers
- ☐ Do you know how long to store both paper and electronic records for every department?

CLASSIFY YOUR RECORDS

- ☐ Do you know how to classify records, either automatically or manually, so that they can be easily stored and accessed?
- ☐ Are your digital records loaded into an Enterprise Content Management (ECM) system?
  - ☐ If so, have you set up retention and destruction schedules to fit your organization's needs?

SECURE YOUR RECORDS

- ☐ Are your records securely stored?
- ☐ Does your records management strategy meet these four basic security requirements?
  - ☐ Physical Security - Are all your paper documents, files, flash drives, and back-ups that contain critical personal information locked in a room or a file cabinet that is secure?
  - ☐ Electronic Security - Are your electronically stored documents protected from attacks and breaches with encryption both during transmission and at rest?
  - ☐ Authentication - Do you restrict user access to information through extensive security settings to control user, project and document settings?
    - ☐ Does your system provide evidence of audit trails, security controls, user activity, and document history?
  - ☐ Disaster Recovery - Is your data secure from theft, loss, natural disaster or cyber attacks?

COMPLY WITH POLICIES

- ☐ Is your organization aware of the federal and state regulations with which you must comply?
- ☐ Have you consulted with your attorney to determine which regulations apply specifically to your industry?
- ☐ Do you have to comply with any of the following:
  - ☐ Sarbanes-Oxley Act (SOX)
  - ☐ Health Insurance Portability and Accountability Act (HIPAA)
  - ☐ Federal Rules of Civil Procedure (FRCP)
  - ☐ Gramm-Leach-Bliley Act (GLBA)
  - ☐ SEC Rule 17 (SEC 17)
- ☐ Do you know the penalties for noncompliance?
- ☐ Are you subject to audits?

ELIMINATE EXPIRED RECORDS

- ☐ Do you know what records you can get rid of?
- ☐ Is the destruction of these records automated or are individual employees responsible?
- ☐ Who are the individuals involved?
- ☐ Can you consistently determine what records can be destroyed?

DIGITECH SYSTEMS

Now that you know what questions you need to answer, getting a formal policy in place will be a breeze.
Contact us if you need help with your plan! • www.digitechsystems.com/rr