IRON MOUNTAIN®

Data Protection

Data Protection Checklist

8 tips to safeguard your business information

1. Structure your data. Understanding what you have and where you have it are two of the fundamentals to any secure information management policy. Poorly ordered data not only detrimentally affects work efficiency, it also increases the risk of loss. Set some structure to how and where files are located. This should include both physical and electronic assets as formal business records which provide evidence of important transactions and decisions.

2. Assess and treat associated data risks. Understanding what risks your information faces allows you to target your efforts of protection and gives you a formal methodology for requesting business support and treatment. A simple assessment to look at the hazards to your business will ensure you protect your information in a compliant and secure way.

3. Ensure you can recover data. This could involve storing server data on tapes at a secure, external archive center. Businesses are also discovering the Cloud as a secure backup solution, especially for data which needs to be accessed at short notice. A Disaster Recovery and Business Continuity plan combined with both forms is generally the most reliable solution.

4. Set permissions for access. Sensitive information access must be meticulously controlled. Model the company's internal security policies by authorizing user information access based on specific permissions or job roles. Ensure these permissions are reviewed in a timely manner.

5. Be aware of statutory retention periods. While the complexity of the associated laws and regulations continues to rise, so do the penalties for infringing them. Keep a close eye on the statutory retention periods associated with your data.

6. All for one, one for all. Get the board behind you to support your information security practices and authorise your polices. Support from the board will make your live easier. Use your risk assessment to demonstrate the tangible risks to the business and give them the information to decide on to accept or treat the risk.

7. Train staff. Staff need to receive regular and adequate training on internal data security rules and statutory ones that exist when handling sensitive data. People are one of the highest risk factors where data malpractice is concerned, but they can also be one of the biggest defence mechanisms your business can operate when skilled accordingly.

8. Expertise. Don't be afraid to seek help. There are a number of organisations out there who can help and support you with your Information security requirements. The best approach, as modeled by the ICO, is to 'Empower, Educate and Enforce' your information security policies. This coupled with the drive of efficiency within your business can lead you to partnering with industry experts to ensure your information management remains compliant and secure.