IRON MOUNTAIN®

THE 3 P'S OF INFORMATION SECURITY & RECORDS MANAGEMENT FOR REMOTE WORKERS

BEST PRACTICES FOR SMALL BUSINESSES

INDUSTRY FACT

"SMALLER BUSINESSES ARE MORE VULNERABLE TO CYBERCRIME, BECAUSE UNLIKE BIGGER FIRMS, THEY ARE LESS LIKELY TO HAVE TEAMS OF IT SPECIALISTS IN PLACE TO PREVENT OR RESPOND TO A DATA BREACH, OR THE RESOURCES TO INVEST HEAVILY IN CYBER SECURITY."

ZURICH INSURANCE UK

With each employee you have working remotely, cracks in the information security foundation can start to spread. Hackers know how to exploit vulnerabilities for financial gain with cyberattacks, ransomware and phishing emails on the rise.

The last thing your small business needs is an added setback as you try to grow. Help your teams manage through any remote work changes with clear communication around information safety best practices.

POLICIES

Provide all employees with clear and concise written policies covering key aspects of information security. This should also include the acceptable use of their laptops, phones, and other devices. As a starting point for remote working security, consider building out company policies around the following:

- Conducting company business on personal computers or phones
- Copying business records to personal devices
- Sending business records to personal email or any other email outside your company domain
- Printing business documents at home
- Using personal flash drives to store business information

The policies don't need to be lengthy. They just need to be clearly communicated, easily accessible, and understandable. In remote work settings, we recommend providing policies in a digital format with multiple points of contact for questions.

PROTECTION

Remote workers need to be extra vigilant regarding the information security on all their devices. Train them to be hyper alert to cyberattacks, ransomware and phishing emails. Warn them that criminals are looking to exploit the spread of COVID to conduct hacking campaigns. Encourage them to use privacy screens to protect their information.

TO HELP MAINTAIN A HIGH LEVEL OF DILIGENT SECURITY MONITORING, HERE'S A LIST OF OUR REMOTE EMPLOYEE DO'S AND DON'TS:

Do	Don't
Use a secure Wi-Fi connection	Use public Wi-Fi hotspots
Store devices securely when not in use to protect from unauthorised access	Share devices or passwords with people in your household or any public space
Save all business documents to your business network	Save business documents to your personal desktop
Avoid printing documents at home	Print documents from home or public locations
Shred or securely store any printed documents at the first opportunity	Throw printed documents in personal or public trash and recycling bins

PRIVACY

To deflect brand and reputation threats, it's imperative to keep personal customer or client data and intellectual property private. Remote employees who handle sensitive records should have formal training in your privacy policies and tools to prevent misuse.

INDUSTRY FACT

"IT'S IMPORTANT TO REMIND EMPLOYEES WORKING REMOTELY, OF BEST PRACTICES FOR INFORMATION MANAGEMENT AND SECURITY. IN STRESSFUL TIMES, PEOPLE FIND WORKAROUNDS, SO KEEP THE COMMUNICATION SIMPLE AND SPECIFIC."

ARLETTE WALLS, GLOBAL RECORDS & INFORMATION MANAGER, IRON MOUNTAIN

WHY IRON MOUNTAIN?

- Bestselling SMB Solutions
- Dedicated account representatives
- 24/7 Customer Service

1300 476 668 | IRONMOUNTAIN.COM/AU
0800 732 255 | IRONMOUNTAIN.COM/NZ

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.