Organizations around the world are facing new and unparalleled challenges related to the COVID-19 pandemic. With so many employees now working from home, Iron Mountain is sharing best practices for maintaining the security and privacy of your information during this unprecedented time.

Whether in a cubicle or your home, how you manage records and data is no different - all employees must comply with organizational policies. Given the circumstances, employees could be preoccupied with managing through the crisis and need clear communication and reminders on policies and procedures.

POLICIES
Ensure policies are available to all employees - remind them where they are located on your intranet. Communicate to all employees - when in doubt, refer to the policies for:

› Records and Information Management
› Security
› Privacy
› HR remote working guidelines
› Device security, including:
  › acceptable use of devices and handling of information
  › records copied to a personal device
  › records sent to a personal email
  › home printer drivers
  › use of flash drives

Be sure to publish contact information to answer questions and address concerns.

SECURITY
While working remotely, employees need to be extra vigilant regarding the security of information and devices.

› Protect your devices from unauthorized access by storing them securely when not in use.
› Do not share devices or your login and password information with people in your household.
› Save all content to your designated network, not to your desktop.
› Information saved to your desktop is not securely stored and protected.
› Refrain from printing records/documents.
› If you do need to print, keep these documents secure:
  › Do not throw your organization’s paper records/documents in the trash or recycle bin.
Retain printed documents in a secure place until you can:

1. Return to the office and place in a secure shred bin.
2. Shred on your personal shredder, according to your organization’s shred-spec policy.
3. Go to a retail outlet that offers secure shredding services.
   - For a list of Iron Mountain’s authorized shred partners in your area, click here (ironmountain.com/residentialshred).

Whether working from home or in a public place (as allowed under COVID requirements) use a secure connection rather than a public WiFi connection.

Use privacy screens to protect your information.

Train your employees to be hyper alert to cyberattacks, ransomware and phishing emails. Warn employees that criminals are looking to exploit the spread of coronavirus to conduct cyberattacks and hacking campaigns.

PRIVACY

If handling/using records with personal data, you must be mindful of compliance requirements; the information must not be made available to any unauthorized people. It is essential that private and sensitive data, as well as intellectual property, are not exposed to any risk of potential data breach or misuse.