5 Guidelines

for Work-From-Home Workers

From a Real Risk Manager

Now, when the coronavirus has forced so many companies to quickly adapt to a larger remote workforce, risk management is more important than ever. Carly Franks, Senior IT Security Risk & Compliance Analyst at Mitratech, has a few policies and procedures that can help us all in working remotely

We can help you mitigate COVID-19's effects

With easy-to-adopt-and-use risk management solutions. Learn more at our Coronavirus Impact Solutions Center.

Learn More

MITRATECH

1. Be aware of your surroundings

- Position yourself to make eavesdropping and peering at screens not possible.
- Ensure devices and company data are secure from unauthorized access, loss, or theft.
- Consider adding security controls if using public Wifi.

2. Be cautious about email use:

- Have a heightened awareness about emails received.
- Be alert to anomalies.
- If it doesn't fit into normal patterns, question it.

3. Use company-issued devices only for company work:

- Never use company equipment for non-business purposes, including:
  - Gambling or gaming
  - Online shopping
  - Entertainment
  - Sites with obscene, hateful, or objectionable material.

4. Be careful with printing, or anything printed:

- Do not throw paper with company business information in the trash can. Instead, save it to be properly destroyed at the office.
- Do not leave document originals on the glass or in a tray of a copier.
- If using a printer others use, clear the buffer of data afterwards.

5. Observe sensible digital security:

- Conduct the company's business using company-issued devices, unless otherwise approved.
- Password protection is mandatory for any company-related work.
- Save all remote work on the company's system or transfer to it ASAP.
- Delete files or data afterwards, if using a required third party IT device
- Immediately report any lost or stolen device with company data.