FIELD EFFECT

Securing remote and hybrid work environments: The definitive checklist

Your workplace has changed. Your cyber security should too.

Whether you have an entirely remote or hybrid environment, employees need access to the same hardware, software, and data without compromising security. This creates a big challenge since cyber risks increase when staff work in new locations.

Use this checklist to learn cyber security best practices that will protect your teams, data, and systems.

- [ ] **Do you have a remote work cyber security policy?**
  Develop and distribute a policy that outlines the cyber security risks associated with remote work, such as using public wi-fi, and safe computing behaviours that reduce them.

- [ ] **Are employees using strong, unique passwords for every account?**
  Employees should choose longer passwords with upper and lowercase letters, numbers, and symbols. We also recommend using passphrases — strings of words that make sense to the user only. Password manager tools can help keep track of complex credentials.

- [ ] **Have you enabled multi-factor authentication (MFA)?**
  Multi-factor authentication takes username and password security further with an extra step to validate the user's identity. This added protection is key for modern work environments, limiting the risk of credential stuffing, brute-force password attacks, and more.

- [ ] **Do employees know about major cyber threats?**
  Make sure everyone understands the techniques and possible signs of common cyber attacks, such as phishing. Education is vital for all staff, but remote workers should know the signs of an attack, including markers of a malicious email, and how to respond correctly.

- [ ] **Are all hardware, software, and cloud applications configured correctly?**
  Ensure all IT infrastructure is configured to optimize cyber security, such as managing user access permissions, automatically applying updates where possible, and more.

- [ ] **Have you developed a bring your own device (BYOD) policy?**
  Set cyber security and appropriate use guidelines if employees use personal and company-issued devices. Specify what devices and applications are allowed, password rules, who owns device data, and more.

- [ ] **Have you implemented a mobile device management (MDM) solution?**
A mobile device management (MDM) solution is a great way to oversee company-issued devices remotely. It helps you implement policies that secure, monitor, and manage mobile hardware, as well as remotely lock or wipe devices if lost or stolen.

- [ ] **Have you set up a remote access VPN?**
A corporate virtual private network (VPN) creates an encrypted connection that enables secure remote access to your network. Configured correctly, a VPN allows employees to safely retrieve, store, and share data from anywhere.

- [ ] **Have you developed appropriate use policies?**
Hybrid work environments require new tools, such as web conferencing and instant messaging, to enable safe productivity from any location. Develop an appropriate use policy outlining how to use (and not use) new company technology.

- [ ] **Are machines set up to encrypt data?**
Encrypting data translates it into a code that's only readable to those with the key, reducing potential device loss to only the cost of the hardware and not the information on it.

- [ ] **Are you regularly backing up data?**
Saving and uploading data using a cloud back-up service ensures that critical data is encrypted and accessible to authorized users only.

- [ ] **Do you provide regular cyber security training for employees?**
Provide employees with regular cyber security training to keep the subject top of mind. It could be as simple as emailing best practice tips or working with a learning provider to deliver online sessions.

- [ ] **Do you have visibility across your IT infrastructure?**
Implement a cyber security solution that monitors networks, endpoints, and cloud-based services 24/7. This in-depth visibility makes it easy to protect devices, assets, and users no matter the location.

Sharing is caring

Please feel free to share this checklist with colleagues or anyone else who may want to learn more about cyber security best practices for modern business. If you have any questions about defending a remote or hybrid work environment, we're here to help. Reach out!

Contact us today.

Email
sales@fieldeffect.com

Canada and the US
+1 (800) 299 8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418