

Checklist for a employer



Security Training:

Provide regular security training with the focus on remote work-related security issues.
Ensure that the employees are aware of the latest threats.

Physical Security:

Provide guidelines to employees for securing their home work environment.
Consider lockable cabinets for sensitive information if necessary.

Passwords:

Encourage employees to use strong passwords and change them regularly.
Provide tools for password management if needed.

Email:

Ensure employees have clear instructions for identifying suspicious emails.
Provide tools for verifying email authenticity if necessary.

Workspace:

Encourage employees to keep their workspace tidy and protect confidential information. Provide secure storage options if needed.

Backup:

Ensure that backups cover remote employees.
Provide company services for backup.

Remote Work:

Provide the secure remote working tools and ensure that the employees are familiar with their proper use. Also regularly check the security of remote connections.

Mobile Devices:

Provide company-approved mobile apps.
Ensure that the employees use mobile devices properly.

Malware Infection:

Establish clear procedures for how to deal with malware infections.
Provide support services and stay in contact with security officers.

Culture of Continuous Improvement:

Encourage open communication and reporting of security observations.

Continuously assess and update company security practices to address the work environment and the changing threat landscape.

Customize these guidelines to fit the specific needs of your company.

Security is a responsibility for all.

