# **CORTAVŮ**

#### 21 SECURITY BEST PRACTICES FOR WORKING REMOTELY IN 2024

Hybrid and remote work has become a standard operating procedure for many companies. To help you maintain a robust security strategy in 2024, we've compiled a list of 21 best practices to ensure your work environment remains secure, no matter where or how you get your job done.





### INSTALL ESSENTIAL SECURITY PROTECTIONS

Ensure all your devices, whether companyissued or personal, are protected by actively licensed antivirus and antimalware solutions.



#### KEEP HARDWARE & SOFTWARE UPDATED

Cybercriminals exploits security vulnerabilities in your hardware and software systems. Always install security patches.



### SECURE YOUR HOME NETWORK

When working from home, make sure you're using a wireless network that is secure and password-protected.



### USE VPN TO ACCESS COMPANY RESOURCES

Using a VPN while accessing company data or applications helps protect your privacy by encrypting all traffic and data transmitted.



#### ENABLE MULTIFACTOR AUTHENTICATION

Multifactor authentication enforces control over who logs in to company applications, protecting against unauthorized access.



#### **SECURE PERSONAL DEVICES**

Implement encryption for data assets and internet traffic if you access company systems with your personal device.



### FOLLOW COMPANY PASSWORD POLICIES

Make sure you are adhering to your company's password policies and criteria requirements to avoid weak passwords.



# NO PERSONAL DEVICES WITHOUT A BYOD POLICY

Using an unsecure personal device for work can expose your company's network and systems to security risks or even data theft.



# ADHERE TO ALL COMPANY SECURITY POLICIES

Follow your company's IT and security policies. This helps you securely access your company's data, network and resources.



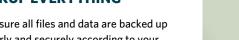
#### **BEWARE OF PHISHING SCAMS**

Security risk is one of the trade-offs of remote work. Read emails carefully before responding and avoid malicious links.



#### **BACKUP EVERYTHING**

Make sure all files and data are backed up regularly and securely according to your company's backup policies to avoid data loss.





### COMPANY-ISSUED DEVICES ARE FOR YOUR USE ONLY!

Never allow anyone to use your companyissued devices that contain private, sensitive or restricted company data or systems.



#### **AVOID USING PUBLIC WIFI**

Public WIFI can expose your device to security risks. If using a public WIFI connection is unavoidable, always use a secure VPN.



### AVOID PRINTING OR WRITING DOWN SENSITIVE INFORMATION

Never print or write down any sensitive or private data. If necessary, keep records securely locked and out of view.



### SECURE ONLINE/VIRTUAL MEETINGS

Use one-time PINs or access codes and MFA to ensure only authorized personnel are attending the meetings.



#### PAY ATTENTION TO PRYING EYES

While working from a public place, pay close attention to prying eyes. Skilled shoulder surfers could easily identify sensitive information and obtain your credentials.



### LOCK YOUR DEVICE OR LOG OUT WHEN NOT IN USE

An unlocked device is an invitation for trouble. Make it a habit to lock your device when unattended.



# COMPANY DEVICES ARE NOT FOR PERSONAL USE

Using company-issued devices for personal activities, such as online shopping, gaming or social networking, puts your company's sensitive data at risk.



# NEVER SHARE PASSWORDS OR ACCOUNT CREDENTIALS

Never share your passwords or login credentials with anyone — colleagues, family members or friends.



### STICK TO COMPANY APPROVED COMMUNICATION

Always use company-provided resources, such as corporate emails and collaboration tools, to communicate or share data.



#### **COMPLETE SECURITY AWARENESS TRAINING**

Make sure you complete the training programs to learn the strategies, measures and actions needed to stay safe.

# CORTAVO

If you need help securing your home working environments, devices or data, contact us today. Make sure that remote workforce security is a part of your cybersecurity strategy in 2024.