ThoughtWorks®

The Remote Work Playbook Series: Privacy & Security

For Organizations

Remote Working Policy

Create a remote working policy to ensure that everyone understands what is expected of them, aligned to the specific requirements and risk appetite of your organization. Within this policy you should include a detailing of acceptable applications and working practices, as well as technical details such as VPN connectivity. If applicable your policy should include handling commercial information as well as personal information considerations.

This policy is where you get to be explicit about exactly what you are happy with. Different companies have different risk profiles, and differing levels of comfort with their risks. Is it ok that people use a personal device for work? Do you want them to take calls within earshot of others? Understanding this context, you will need to make some decisions for your organization.

Communicate

For your policy and other guidance to be effective, you need to communicate using all your available channels. Word of mouth won't be working as well at the moment, so issue your updated policies and guidance through your intranet, email, and other digital communication channels such as Slack, Google Hangouts, or Teams. Keep republishing them, with an eye on read rates.

Useful Information to Communicate:

- How and when to use the company VPN
- Which tools are approved or blacklisted
- Best practices for using collaboration tools
- IT Security policies and guidelines
- Where to get support
- The remote working intranet page

Training

Use the opportunity to provide a refresher to colleagues on privacy and security including appropriate levels of access, and any additional security settings that tools may provide. Additional training materials are being provided for free at this time - make sure to use these resources if you don't have internal training.

Make It Simple

If doing the right thing is close to doing the most convenient thing, then you are going to have high levels of compliance. Ensure that your compliance practices are not overly clunky otherwise they are not likely to be followed.

Accessible Front Door

Ensure there is a well communicated front door to your essential processes, as people are no longer going to be able to walk over to the person they know in IT to help fix their devices, or report an issue such as a phishing email or a potential breach. This could be as simple as a form on your intranet or an intuitively named support email address.

Consider whether you want a simplified and dedicated process for requests around remote working, or if you'd prefer to use well established channels, with extra hands and expedited mechanisms in place to support additional volume and urgency. The more you can enable self service for people, the less demand on your support teams.

Device Security

To protect your computer devices from online threats as well as device loss, all should have the following controls in place:

- Anti-virus program
- Local device passwords should be strong, unique, and random
- Full disk encryption should be enabled
- Mobile Device Management (MDM)
- System auto-patching enabled
- System firewall enabled
- Find my Mac enabled
- Idle machine lock

Endpoints

Your organisation may not provides laptops by default. In this case, you're going to have to make a decision on who most needs the available company laptops. Consider if there are those that can relocate desktops from the office, if there's a need to buy new devices, or if you want to approve the use of personal devices.

Decide which applications are to be made available, to whom and how, and what is the expected device security stance for each combination, and make this information available. This approach allows decisions that balance business risk with compliance risk.

Authentication controls

Don’t make secure authentication hard. People will take shortcuts, reuse passwords or use patterns. Make it easy for people to do the right thing.

Ideally you already have a Single Sign On (SSO) product, paired with Multi-Factor Authentication (MFA). If not, it’s worth considering, but now is not the time to kick off a big implementation project. A reasonable short term alternative is to provide a password manager, which will make life easier and safer for both individuals and companies. Many of these products are currently offering limitless trials for businesses.

Passwords and MFA

Review your password policies, the latest standards, propose longer minimum password lengths, without complexity and without short cycle times are more secure than shorter passwords, with complexity requirements.

Make sure people have more than one MFA option, to reduce the chances that people will be locked out.

The gold standard for authentication is modern passwordless authentication. This approach uses cryptography, is very secure and reduces friction for people. It also has the potential to reduce support demands, protect against phishing and man in the middle attacks. It is often combined with machine learning and can be set up to recognise unfamiliar devices, login locations or impossible travel scenarios, prompt for additional verification or even deny access in a high risk situation.

For Individuals

Access Controls

As we move away from post-its, whiteboards, and face-to-face conversations to online collaboration, we need to be careful regarding who has access to that information:

- Ensure that you regularly review who has access to your shared working environments like Jira, Trello, Github etc.
- Make sure you understand the different kinds of sharing options in your collaboration tools and team drives; whether they are network shares or cloud services like Google Drive or OneDrive. Verify that the sharing settings only allow access to the right people.
- Be vigilant in video calls: ensure the audience is who you expect. Consider adding a password to your video calls or other equivalent security such as enabling the waiting room feature (Zoom, Webex, Webex PRs). Query people you don't recognize - just like if there was a stranger in your office.

Sharing Information

Confidential conversations (commercially sensitive or containing personal identifiable information) which would have taken place face to face are now taking place electronically. This brings extra responsibilities regarding data security as well as records management.

- Ensure that you send these via secure means using your organization's approved tools, and only use personal devices if they have been approved by your organization.
- Publicly available messaging tools like WhatsApp, Facebook Messenger and WeChat should not be used for sharing commercially sensitive or personal information. Use the platforms that your organization has provided.
- Avoid sharing personal information over chat (e.g. MS Teams, Slack or Hangouts Chat) or email. If you need to share, put it in a document that is access controlled and then send the link. This will let you un-share it if needed, and avoids the risk of it being copied or shared further outside of your control.
- Where email is your only option, consider using confidential mode (Gmail, Office365).

Mobile Messaging

Taking the above advice into account, non-confidential conversations can occur via your usual digital channels, including on your personal devices where there is no practical alternative and the benefits outweigh the risks. Be extra wary of tools which haven't been provided by your organisation.

Secure Connection

Ensure your internet connection is secure. Protect access to your home network with a strong password. Make sure your home internet routers and modems are secured with strong admin passwords and kept up to date with latest firmware.

Publicly available wi-fi, such as in hotels and cafes, is not generally considered secure. Use a VPN if your organization has provided one, especially when using public networks.

Personal Devices

Different organizations have different policies regarding personal devices (aka "Bring Your Own Device") and endpoint security. Make sure you follow these policies and only use approved devices. In exceptional circumstances, such as your work laptop no longer working or your organization not yet issuing laptops, ask your IT and Information Security Teams what your options are.

As a rule, avoid using your personal devices when handling confidential information. Ensure your device has a password or similar lock (e.g. fingerprint/facial recognition), and enable encryption if possible.

Beware of Scams

Unfortunately in times of crisis scams rise as people's appetite for information increases.

Be mindful of phishing attempts: we've seen some very elaborate Spear Phishing and Whale Phishing attacks where the perpetrators pretend to be senior executives asking for urgent favors via email and also using many social platforms. Thanks to information easily found on LinkedIn and other sites, these can be very convincing.

Any requests from people to expose data, provide additional access, click on a link, or result in the transfer of money or assets should be given extra scrutiny.

Label Your Devices

If you are working in a space with other people such as flatmates or family members who may have similar looking laptops, drives, and other items, put a post-it note on your devices to ensure there are no mix-ups.

Screen Security

If you work in a shared space, lock or close your screen when you are not using it. Ensure that a password is required to wake up your device after inactivity.

Consider using a privacy filter to protect the information you are working on on your screen.

Physical Security

Keep your devices and documentation physically safe by ensuring that you lock it away at night at your home if this facility is available to you, if not then store in a safe place out of sight, on your premises.

Do not share work computers with anyone else in the home. This will help reduce the risk of unauthorized or inadvertent access to protected company or client confidential information. If you are working on a personal or shared device, use Chrome Profiles or Firefox Containers to keep work and personal information separate.

Avoid storing information on portable hard drives and USB drives which can easily go missing. If you do need to use one, ensure it's encrypted and has a strong password. (Mac, Windows)

Report Issues

If you see a potential phishing email, tech issues or which are causing you to use unusual work arounds, or a potential breach, report these through the same channels you would if you were in office, or the communicated remote alternative.