JCJ – P.A.T.T.I Q

Remote Work Framework

Table of Contents

[Executive Summary 3](#_Toc69145808)

[Introduction 3](#_Toc69145809)

[Plan 4](#_Toc69145810)

[Vision & Mission 4](#_Toc69145811)

[Policies & Procedures 4](#_Toc69145812)

[Standards & Guidelines 4](#_Toc69145813)

[Legal 4](#_Toc69145814)

[Training & Tools 5](#_Toc69145815)

[Architect 6](#_Toc69145816)

[Vulnerability Management 6](#_Toc69145817)

[Data Security 7](#_Toc69145818)

[Collaboration Tools 7](#_Toc69145819)

[Remote Access / VPN 7](#_Toc69145820)

[Corporate Infrastructure 7](#_Toc69145821)

[Train 9](#_Toc69145822)

[Home Internet 9](#_Toc69145823)

[Passwords & Security 10](#_Toc69145824)

[Physical Security 11](#_Toc69145825)

[Phishing 12](#_Toc69145826)

[Test 13](#_Toc69145827)

[Device Security 13](#_Toc69145828)

[User Access 13](#_Toc69145829)

[Security Controls 13](#_Toc69145830)

[Ensure CIA 14](#_Toc69145831)

[Implement 15](#_Toc69145832)

[Multi-factor Authentication 15](#_Toc69145833)

[Awareness 15](#_Toc69145834)

[QA 15](#_Toc69145835)

[Validate 15](#_Toc69145836)

[Document 15](#_Toc69145837)

[Monitor 16](#_Toc69145838)

# Executive Summary

JCJ Alliance is a group of cybersecurity professionals who have created this open-source framework to streamline the process of converting your On-Premises employees to Work-from-Home employees. We understand how this may present a challenge to organizations that may lack the policies, technology, and training to secure a remote workforce. We also understand, from experience, how employees may be unfamiliar or uncomfortable with the idea of working from home. The purpose of this framework is to provide security concepts to be discussed by your company’s Information Security and Information Technology teams. We recommend you focus just on the most important concepts that will have the greatest impact on your organization and implement the processes that will help maintain your company's Confidentiality, Integrity, and Availability while your employees are working off-site.

We have designed these concepts with a focus on the financial industry, but we believe this framework can easily be adopted by Cyber Security professionals across all industries. We hope this strategic framework helps to address your most pressing security concerns related to creating a work-from-home workforce and makes your conversion process as simple as possible.

Introduction

With the coronavirus disrupting business as usual, financial organizations worldwide are implementing work-from-home policies. Not only does this pose new challenges for organizations that lack the processes and technologies required to secure a remote workforce, it puts an even greater burden on families who must quickly adapt to a new way of working and learning from home — and do so safely and securely.

We have created a framework to provide step-by-step guide on how to implement a remote security initiative across your organization with quick tips, best practices and newsletters for individuals and families. The P.A.T.T.I Q Remote Work Framework covers everything you need to know to Protect your business and your family.

# Plan

## Vision & Mission

Reimaging your vision and mission

As a good builder, you need to start from the foundations; the company’s vision and mission. Now that remote work is the norm, your employer branding will benefit from a tweak. You can brush it up and reconstruct it by prioritizing the new values you’d like to embrace. Flexibility, adaptability, and agility are some of them.

Policies & Procedures  
Create a policy that is tailored to the needs of remote employees. Not all jobs should be done outside of the office. Any position that works from home will benefit from the policies and procedures you develop.

<https://resources.owllabs.com/blog/remote-work-policy>

Standards & Guidelines

Set goals to make sure your remote workers have the tools they need to carry out. The following is some best practices to help with productivity, organizational skills, and well-being:

* Be sure that all remote employees have access to the systems, programs, and tools that are normally used to perform their duties. Evaluate if sufficient protection and data privacy are in effect when accessing, sending, receiving material, and including paper copies of records they may have at home.
* Remote workers should create a comfortable, functional workspace, that minimizes at home distractions.
* Create a system for tracking and approving hours. If handling non-exempt workers, be sure they let management know when they’re going to take a break.

Legal

Clearly outline the legal rights that remote workers have.

Remote workers are entitled to the same legal protections that in-office workers have. However, working remotely can present some added challenges that need to be addressed to ensure your company is legally compliant.

Set up a process to report hours for hourly remote workers. If they work more than 40 hours, they'll likely qualify for overtime. To avoid high overtime costs, select times that employees should and shouldn't be working. With clear guidelines, they won't be able to work outside of these hours unless they have permission from their manager. This makes it easier to avoid employees accidentally working more hours than intended.

It's important to support employees that are remote just as you would in-office workers. This means clearly discussing the training, benefits, and promotions that are available to them. If you don't provide remote workers with the same level of assistance as in-office workers, it could result in discrimination or disability-related workplace violations. (Barbara Z. Larson, 2020; Risto, 2020)

<https://www.jdsupra.com/legalnews/best-in-law-remote-working-laws-for-42015/>

Training & Tools

Provide the right tools for successful and secure work.

When working away from the office, your employees need the right tools to work securely and productively. For many employees, a laptop and a Wi-Fi connection might not be enough. Remote employees need technology that makes them feel engaged and part of the team, not just an afterthought.

Additionally, cybersecurity concerns should be top-of-mind. Remote workers might need a VPN or another form of security to work on important company files or private customer data. And while some employees might be able to operate using public Wi-Fi networks, others might need to stay at home or in a more secure co-working space to ensure data privacy.

You'll also need policies and tools in place for remote team collaboration and communication. Use additional tools like live chat, synchronous screencast recording, live video conferencing and more to ensure technology doesn't get in the way of an effective and meaningful work relationship.

Architect

Many companies do not have the resources to architect, design and build their own programs from scratch. Fortunately, there are several mature frameworks that can be used as references for this purpose. The National Institute of Standards and Technology (NIST), SANS, and Center for Internet Security are all great references for building your Information Security program.

Now that you have scoped the project of working remotely you will need to consider what is needed to make that a reality. Many of the requirements should already be in place but must be evaluated to ensure that are properly sized. Consider the factors below to help determine any gaps you must fill before transitioning workers.

Vulnerability Management  
Vulnerability Management is necessary whether your organization allows remote work or solely works from the office. There are several frameworks that cover Patch and Vulnerability Management. At its core vulnerability management is used to keep systems up-to-date and reduce the risk of computing resources. Two of the most recognized and followed are from The National Institute of Standards and Technology (or “NIST”) and SANS Institute.

NIST’s Enterprise Patch Management is documented in NIST SP 800-40 Rev. 3

<https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>

The SANS vulnerability Management Framework is made up of five parts. They are PREPARE, IDENTIFY, ANALYZE, COMMUNICATE, and TREAT. These are the five areas of the PIACT process from the course. Tasks and activities that are part of a vulnerability management program fit across these five sections.

Prepare:

This focus area is dedicated to what we need to make sure is in place for a successful vulnerability management program. In this section, we have two sub-areas: Policy & Standards, and Context.

Identify:

This focus area comes down to how do we find the vulnerabilities within our organizations. We have three sub-groupings in this section: Automated, Manual, and External.

Analyze:

This section is all about the data: how to look at, categorize, and prioritize the identified vulnerabilities. This section has two sub-areas: Prioritization and Root Cause Analysis (can you tell we have done project management before?).

Communicate:

Once we have the information in hand, this focus area comes into play. We take all the data we have and pass it along to others that need it, in a useable format. There are two sub-groups here: Metrics & Reporting, and Alerting.

Treat:

Finally, the part where all the work gets done to fix the problems we have. The three sub-areas are Change Management, Patch Management, and Configuration Management. (Risto, 2020) (Risto, 2020)

Below you will find a visual summary these five parts of the process.

image.png

Diagram

Description automatically generated

Data Security

As with many other aspects, securing corporate data is extremely important whether you have employees working remotely or not. Ensuring security of your data relies with proper access restrictions and encryption. Data should be encrypted both in-transit and at rest.

Collaboration Tools

Make sure that you have chosen which tools are acceptable for collaborating. Many users already have Zoom or other collaboration tools installed. To ensure security of your data, you will want to leverage corporate approved solutions whether its Zoom, WebEX, GoTo Meeting or another tool.

Remote Access / VPN

There are many solutions available for remote access. You may already have a remote access or VPN connectivity available for your staff. Directing users to login to a Virtual Desktop environment (such as Citrix VDI, VMware Horizon, or Microsoft VDI) can greatly increase your ability to maintain data security since these solutions allow users to connect to a device that is within your infrastructure already adheres to you patch management and security policies.

## Corporate Infrastructure

When considering a remote work strategy additional infrastructure may be required. At a high level you will need to consider the following factors:

* Compute Resources
* Software Licensing
* Network Bandwidth
* End user device strategy

Train

Training will be a crucial part of successfully converting your On-Premises

employees to Work-From-Home employees. Not only will you have to provide

information and resources to help your staff utilize new applications and services,

but you will also need to ensure that your employees understand their role in

helping to keep your company’s networks and data secure.

Be sure to provide adequate training for the new applications required to work

remotely. Make sure that your users have easy access to training and resource

materials for new applications and services. Inform your staff that there will be an

increase in spam and phishing attempts. Educate them on ways to stay vigilant to

spam and fake news. And advise them that attackers may acquire detailed

information about their families and histories so that phishing can be more

convincing.

Home Internet

Researchers at San Francisco State University recommend internet speeds above 5

Mbps as speeds below that benchmark are not adequate for two-way interaction on Zoom.

For glitch-free video meetings, they recommend at least 20 Mbps download and 3

Mbps upload speeds.

The best internet speed for working from home depends on the user's job function.

If a user frequently downloads and uploads large files and participates in video

meetings, ideally at least 25 Mbps is recommended. Conversely, if the user will not

be downloading large files or participating in Zoom meetings lower Mbps should

suffice.

If you are not sure how much speed you need — or even how much you are

currently getting — you can use the speed test and quiz below to gauge your

situation.

[https://athelp.sfsu.edu/hc/en-us/articles/360050514614-Internet-speed-and-](https://athelp.sfsu.edu/hc/en-us/articles/360050514614-Internet-speed-and-%20%20bandwidth)

[bandwidth](https://athelp.sfsu.edu/hc/en-us/articles/360050514614-Internet-speed-and-%20%20bandwidth)

<https://www.speedtest.net/>

Here is how much internet speed some of the most common work apps require:

Graphical user interface, table

Description automatically generated

Passwords & Security

We are living in a technological world where passwords alone are no longer a sufficient means to protect our valued information. Weak passwords continue to be one of the primary drivers for breaches on a global scale. A password by itself is a single form of authentication – if someone else has a user’s login name and password, they potentially have access to all resources that the specific account has access to. Educate your staff on the four key behaviors that can help mitigate brute force or password cracking attempts.

Multi-factor authentication (MFA), also referred to as two-factor authentication, [is a security enhancement that requires a user to provide additional pieces of evidence before logging into an account](https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication). Ultimately, MFA helps prevent unauthorized access to the protected account if your credentials become compromised. If you are not currently using MFA in your log in protocol, consider implementing an MFA enhancement to reduce the risk associated with passwords falling into the hands of an attacker.

According to Microsoft’s blog, [enabling MFA can reduce account compromise up to 99.9 percent](https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/) bringing the chance of stolen credentials down to almost zero.

<https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>

* Using Passphrases
* Unique passwords for all accounts
* Password Managers
* MFA (Multi-Factor Authentication). Often called Two-factor Authentication or Two Step Verification

Use the resources below to educate your users on the best practices regarding password management.

<https://ssahub.sans.org/folders/19qytvyc>

<https://ssahub.sans.org/workspaces/1233465/files/2410166246>

<https://ssahub.sans.org/workspaces/1233465/files/2410166256>

<https://ssahub.sans.org/workspaces/1233465/files/2410166262>

<https://ssahub.sans.org/workspaces/1233465/files/2410166254>

Physical Security

Physical security for your business should remain a priority while you are off-site. Remote technologies and capabilities in the security space are more prevalent than ever before and utilizing these options can help give you peace of mind as you continue your remote work. Consider utilizing remote security technology like, Intrusion Systems, Access Control Systems, and Video Surveillance Systems to help secure your facility and maintain the health of your systems without ever stepping foot on-site.

Also, it is necessary for all those who are working from home to take some of the security measures to safeguard their confidential data. Below are a few tips that could be helpful for IT professionals and your staff.

* If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked — including any mobile phones you might use to check email or make work phone calls.
* If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Do not tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
* If you cannot carve out a separate workspace in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen but will also help to separate your work life from your home life.

Phishing

One of the greatest risks remote workers will face is social engineering attacks. Social Engineering is a psychological attack where attackers trick or fool their victims into making a mistake, which will be made easier during a time of change and confusion. The key is training people what social engineering is, how to spot the most common indicators of a social engineering attack, and what to do when they spot one. Be sure you do not focus on just email phishing attacks, but other methods to include phone calls, texting, social media or fake news.

<https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/>

<https://ssahub.sans.org/workspaces/1233465/files/2410165696>

<https://ssahub.sans.org/workspaces/1233465/files/2410165704>

<https://ssahub.sans.org/workspaces/1233465/files/2410165706>f

Test

All your users need to engage in a “pretend it is real” run-through. Once they are configured, they need to test performing all their job functions working from home to be sure everything performs as expected. Solve problems that come up. If one user has an issue, take preemptive action to be sure it does not happen with the others. This transition is too important to not test out ahead of time.

Device Security

It is necessary for all those who are working from home to take some of the security measures to safeguard their confidential data. It is one thing for a personal Instagram account to be hacked. But leaking your employer’s sensitive data due to an unsecure network? That is a much more serious problem for your company. Taking steps like encrypting your Wi-Fi signal, updating your router’s firmware, and using a [VPN (virtual private network)](https://www.allconnect.com/blog/what-is-a-vpn) are essential to keeping your work life secure.

Below are a few tips that could be helpful for IT professionals and your staff.

* If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked — including any mobile phones you might use to check email or make work phone calls.
* If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Do not tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
* If you cannot carve out a separate workspace in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen but will also help to separate your work life from your home life.

User Access

Confirm users can access the remote resources.

Engage one user from each team to perform a “pretend it's real” run though. Provide a checklist of services and applications the user will need to validate.

Security Controls

**Separate work and personal devices**

It is important to make boundaries between home life and work life while WFH. Use different devices for work and home.

**Use encrypted communication service**

While working from home, your staff will be required to communicate with your teammates and co-workers. Make sure all your digital communications are end-to-end encrypted so that no one else apart from the intended user can get access to your company’s confidential information.

**Employ the Principle of Least Privilege**

An effective method to mitigate security risk is to limit the privileges of your staff. This approach, known as the principle of least privilege, dramatically eliminates the risk of a severe data breach by limiting excess. As a precaution, we recommend having all employees use standard user accounts for routine tasks. Only give superuser privileges to trusted members of your IT team and have them only use these accounts to perform administrative duties when absolutely necessary.

**Remove Orphaned Accounts**

Orphaned accounts are problematic because they are old user accounts that contain data encompassing usernames, passwords, emails, and more. These accounts generally belong to former employees who have moved on from the company, but their accounts might still be on your network and remain accessible.

Ensure CIA

It is essential to maintain Confidentiality, Integrity, and Availability while working from home. The crucial aspect to take into consideration is that organizations should ensure that the Confidentiality, Integrity, and Availability of their systems remain intact. This can be done using the following methods:

* Instead of opening connectivity to employees by connecting to external IP addresses, which allow access to web applications or other systems, organizations could make use of the following:
  + Utilize a VPN that uses proper encryption over the end-to-end connection. Robust encryption algorithms would include RSA 2048-bit and stronger, as well as AES 128-bit or stronger. Other algorithms are still allowed, but it is best not to take any chances.
  + Instead of only utilizing standard authentication with either a pre-shared key (bad idea) or username and passwords that can be compromised through brute force attacks, implement multi-factor authentication (MFA). Implement it at the edge of your network to ensure you make it harder for cyber-criminals to gain access to the environment. You wouldn’t want attackers to gain access to the VPN, which already provides them access to your network. This might happen if you manage your MFA on a bastion host or individual systems. There are always methods to bypass MFA if you can gain access to routers or firewalls that are not always protected with MFA.
* Once connected to the corporate network, utilize the least privileged access. If a set of user credentials are compromised, the attackers will have minimal access to confidential data.
* Increase the log monitoring activities and look for abnormal behavior. This will be more difficult now since there are a lot more connections to the environment from an external perspective than usual.
* Change the way you perform threat analysis. Focus on ways to narrow down your dashboards and alerting. Unnecessary alerts will blur the identification of actual attacks.
* Before systems connect, ensure you have policies implemented that all systems shall be up to date with their patches and anti-malware definitions. Have your anti-malware application scan on access to ensure that systems can identify malicious software immediately instead of when it does its weekly scan.

Implement

Multi-factor Authentication

Implementing Multi-Factor Authentication (or “MFA”) can greatly reduce account compromise. If a user’s password is stolen it is of no value without an additional factor. There are many vendors offering MFA solutions. You may find that you will need more than one to cover all resources since some applications or vendors may only allow use of specific token provider.

What is MFA anyway? MFA refers to entering a username along more than one “factor” to gain access. The main factors are:

* Something you know (*examples:* A *password or PIN)*
* Something you have (*examples: A smartcard, a security token)*
* Something you are (*examples: A fingerprint, your iris, your voice)*

Another factor can be location, such as IP address or geo-location.

.

References:

<https://www.rsa.com/en-us/blog/the-language-of-cybersecurity/what-is-mfa>

<https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

<https://fidoalliance.org/fido2/>

<https://www.yubico.com/authentication-standards/fido2/>

## Awareness

Security is everyone’s job. When companies shift how personnel are allowed to connect to corporate resources, they must also keep in mind how those changes impact your security posture. This is where the training program comes into play. Users must be aware of different factors when working remotely. If at home, they should keep in mind their WiFi security. Whereas in the office or connecting from another location they should be aware of who may be around that can view their screen or might have access to their personal belongings.

# QA

## Validate

Once you have staff working from home you will need to verify that the user experience essentially mimics being in the office. In some cases, this could mean having to hardwire devices to you users’ home router. Other situations could require upgrading internet service.

## Document

Documentation is an important and often overlooked step. Confirm that all documentation is complete prior to closing out the project. This should include everything from the Statement of Work, to Policies & Procedures, Standards & Guidelines, Training materials, detailed architectural documents, and issues with steps taken to resolve.

IT architecture diagrams should include network diagrams with IP addresses, ports, applications, services, and accounts.

All documentation should be reviewed during the QA phase to confirm that changes during the implementation are accurately reflected.

## Monitor

Network logs should be reviewed to confirm that any new vulnerabilities are being blocked and new, legitimate, traffic is being allowed.