



WORKING FROM HOME?

# Set **IT** up so you can **flourish**

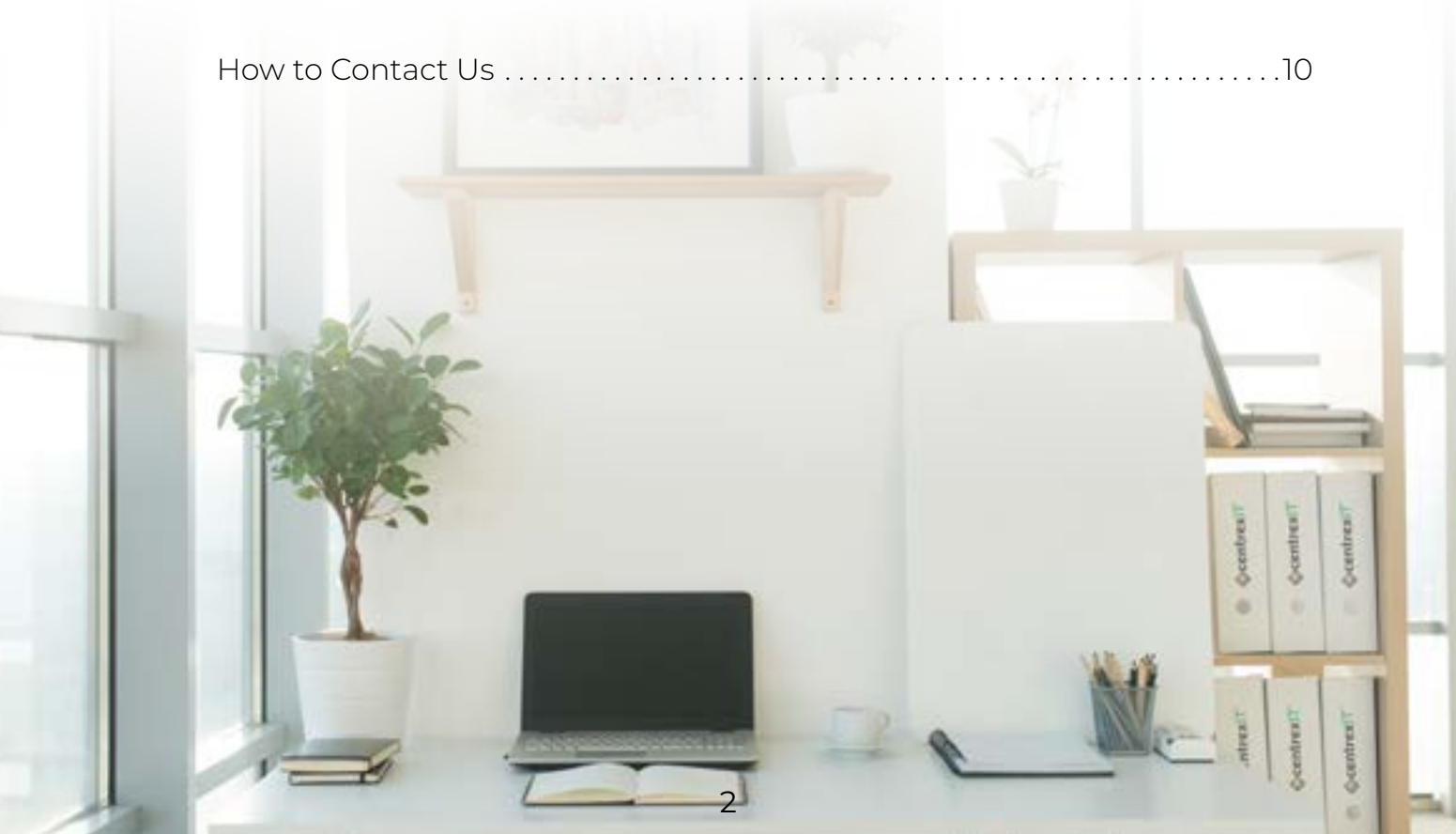
How to empower employees with IT tools to stay  
productive & safe in a remote working environment



# Welcome **Remote** Workers

Here are some tips to help you adapt quickly to remote work by improving your remote collaboration experience and establishing a secure and productive technology environment.

Working Remote: A Shift in Approach .....	3
Business Back-end & Security.....	4
Remote Security Checklist .....	5
Best Practices & Habits to Stay Productive .....	6
What Does Fully-integrated Collaboration Look Like?.....	7
How to Run an Effective Online Meeting .....	8
Top Video Collaboration Tools.....	9
References .....	10
How to Contact Us .....	10



# Working Remote: A Shift in Approach

Working effectively from home isn't just a matter of grabbing a computer and setting it up on your dining room table. Without direct contact with others, the style and types of communications you have need to shift in order to become a work from home (WFH) powerhouse.



## The Remote Experience

### Time & Flexibility

Working from home saves time: from the flexibility to work around appointments to the time saved from cutting out a daily commute.

### Productivity

Many people find that focused work is easier in a WFH environment because they can cut out interruptions from coworkers. In fact, 76% say they always avoid the office in order to work on projects requiring deep concentration.<sup>1</sup>

### Customized Working Environment

To a certain extent, the home environment is more customizable than an office environment depending on what kind of investment you want to make in your personal space. Customizations can lower stress and improve concentration.<sup>2</sup>

### Collaboration & Communication

Many people find it challenging to effectively communicate and collaborate while not face-to-face with another person, which is why video collaboration platforms are such a powerful tool in the WFH arsenal.

### Relationships & Loneliness

Checking in with coworkers regularly and dedicating time for socializing helps the WFH employee continue building relationships and combating loneliness.

### Security Challenges

Security for the remote employee has a long list of challenges (detailed on next page). Always identify needs before letting someone WFH to avoid new security risks.

## Technical Solutions

### The Versatile Laptop

Now powerful enough to accommodate most computing needs, the benefit of having a laptop is that you can work wherever there is a reliable Internet connection. Set yourself up at home with a traditional Internet router, or on the road with a portable hot-spot.

### High-quality Audio Equipment

Don't let poor audio get in the way of effective communications. Make sure you have a reliable phone connection, or if using computer audio for calls, invest in a dedicated headset in order to set you and your company up for success.

### Dedicated Visual Equipment

People receive 80% of messages via body language.<sup>1</sup> In the world of Online video collaboration, having a detached webcam with good lighting can set you apart when speaking with clients.

### Network Folders and Cloud Applications

Network folders for your files (accessed through a secure VPN, of course) ensure your files are secured, backed up, and in shared locations when collaborating with other team members. Cloud applications allow employees to securely connect and collaborate with their colleagues, no matter where they are in the world, as long as they have a reliable Internet connection. And remember, standardize all file storage naming and structure before you start to ensure effective collaboration.



# 75%

of job success is how you connect with other people<sup>1</sup>

# Business Back-end & Security

Don't open yourself up to risk: all access to company data when outside of company-affiliated locations needs to be securely facilitated and controlled by both internal policies and IT security best practices.

## Hardware & Software

### Virtual Private Networks (VPNs)

A VPN puts a strong hedge of protection around home connections, keeping your interactions with the internal network – from emails to confidential data access – secure.

### Anti-Malware & Security Software

All Devices connected to the company's internal networks must be equipped with the managed up-to-date anti-malware and the company's other cybersecurity software. BYOD devices must comply with this requirement before connecting to the network.

### Full-disk encryption

Ensure the company's data is not accessible even if the device falls into the wrong hands.

### Content Access Management

While inappropriate sites are usually blocked when operating on the company firewall, what happens when work devices are used beyond your company's LAN perimeter? Put measures in place on the work devices themselves to prevent unwanted access to certain sites and ensure that no matter where devices are used, restrictions remain in place.

### Cybersecurity Monitoring

Monitor threats and systems in the WFH environment on an ongoing basis to improve security and performance. Remote access and VPN usage should be logged and monitored in a central database and reviewed regularly to detect anomalies and manage remote access privileges.

## IT Security Policies & Practices

### Training

Train each member of the remote workforce on security and home-working policies before deployment.

### Home-Working Policy

Clearly communicate home working policy to workers - it is important that employees are fully aware of their rights and responsibilities before connecting to company resources remotely.

### Automated Technical Security Policies

Many threats can be prevented by implementing technical policies that enforce strong passwords, automated session log off after a set amount of idle time to prevent eaves dropping or accidental data corruption, automated security update installations, etc.

### Single Sign-on

Single sign-on through companies like OneLogin provide both security and user management benefits, such as ease-of-provisioning.

### Multi-factor Authentication (MFA)

Verifying the identity of users with multi-factor authentication and other identity and access management solutions ensures that the right individuals have access to the right resources at the right times for the right reasons.



Microsoft reports that 99% of account hacks are blocked using multi-factor authentication (MFA).<sup>3</sup>

## Remote Security Checklist<sup>4</sup>

- Is multi-factor authentication (MFA) enabled? Did employees receive guidance on how to use MFA (and authenticator apps, if applicable)?
- Is conditional access enabled and configured?
- Do you have the ability to remotely wipe company data from lost or stolen laptops and mobile devices? Are you using whole disk encryption to encrypt the physical hard drive of company laptops?
- Do you have an email security product in place? Were employees trained to recognize and report phishing attempts?
- Have you installed a web security app to prevent users from visiting malicious sites?
- Have you set up data loss prevention policies and/or set applicable restrictions on external file sharing?
- Have you created a remote work and data protection policy for employees to sign?
- Have you conducted end user training on remote security policies and best practices?
- Do you have endpoint protection installed for all remote machines?
- If you are subject to compliance regulations, do you have policies and procedures in place to ensure compliance? Are employees trained to enforce those policies?
- What is your incident response plan during times of company-wide remote work?



# Best Practices & Habits to Stay Productive

It takes effort from both employees and employers to set up a person or team for WFH success.



## Employees

### Time Management

Managing time while remote is critical to keep your working hours effective. Block out designated time for phone/video calls, checking email, and for projects that require deep, uninterrupted concentration.

### Structure & Self-Discipline

It's easy to let personal and work life bleed into each other, but when we do that we don't give our best effort to either. Define a structured schedule based on your particular type of work and set daily, weekly, and monthly goals to keep on track.

### Define Your Workspace

Defining your workspace also does a lot to help keep your work and personal life separate, whether it's in a designated room or simply a corner of the dining room table. Another tip: provide clear guidance for other people you might live with about how to treat you when in your work space to minimize interruptions.

### Always Set Your Status

Let co-workers know your availability by setting your status to "do not disturb" when you are away from your desk or it's outside of working hours. That way, they will not expect an answer right away and you can keep a healthy separation between your personal and working time.

## Employers

### Implement Key Performance Indicators (KPIs)

Everyone needs some sort of KPI to gauge how well they are accomplishing their tasks. When you or your boss are remote, KPI help both of you determine if the work is getting done as-expected and on-schedule. Clear expectations can reduce stress and help with overall job performance.

### Regular Meeting Cadence with Team

Regular departmental meeting cadence builds strong relationships between team members and keeps projects on track.

### Manager Check-Ins

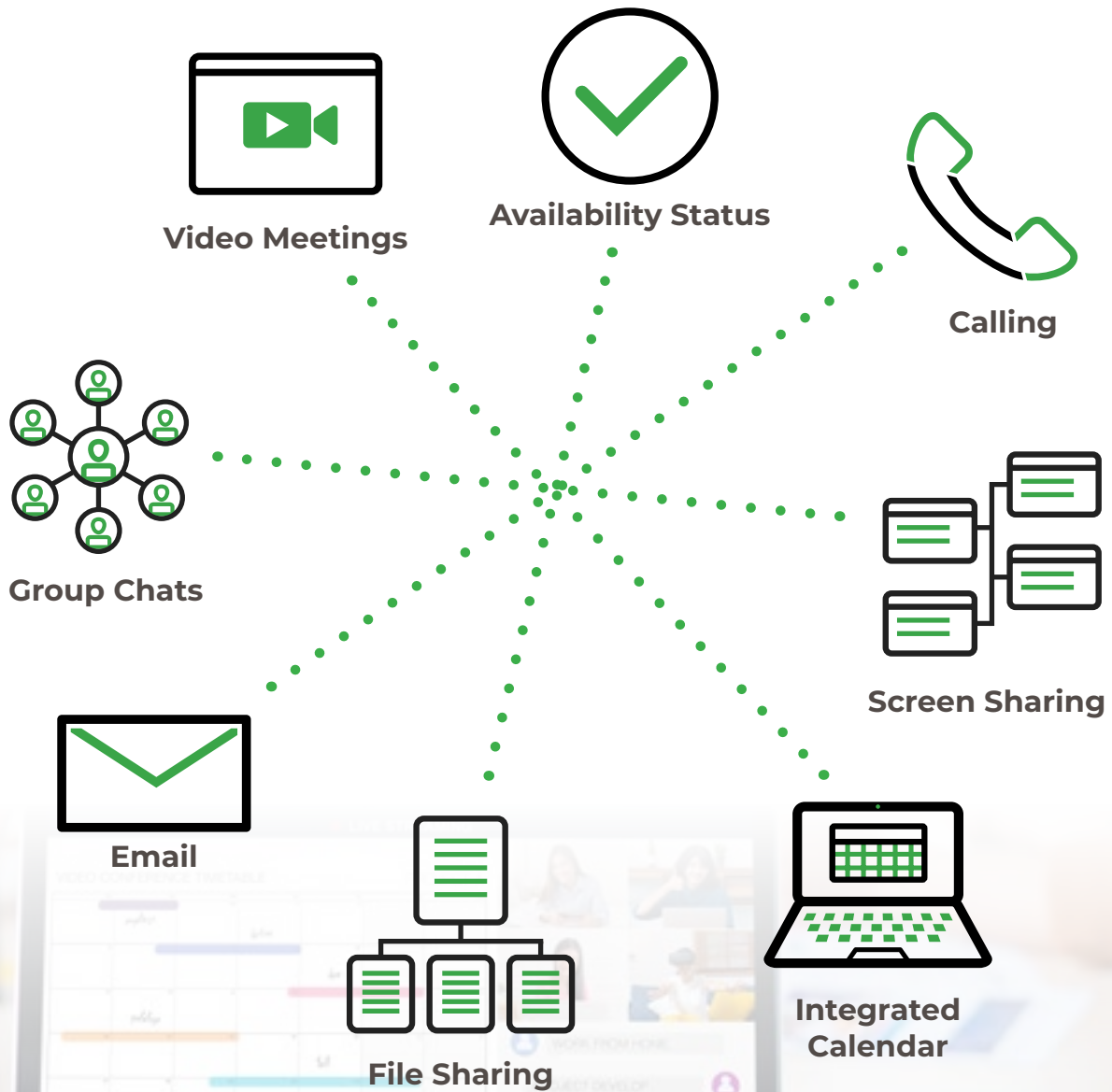
Managers should plan to check in regularly with each member of their team. The frequency depends on the type of work involved and the working style of the employee.



### Productivity Hack

Working when you are at your most productive can increase your output and decrease stress. For best results, create your working schedule based on your concentration types during different times of the day.<sup>5</sup>

# What Does Fully-integrated Collaboration Look Like?



## How to Run an Effective Online Meeting

Running an effective Online meeting follows similar guidelines of running an effective in-person meeting, with some additional practices that keep things smooth in the face of technological bumps or missteps.

Some challenges of Online meetings include: not being able to hear people properly because of poor audio quality, attendees experiencing a poor connection to the meeting, and not having a clear understanding of proper Online meeting etiquette. Understanding the extended roles of the Online meeting Host helps with these challenges.

### The Online Meeting Host

The duty of the meeting Host is to ensure that the meeting runs smoothly and stays on-topic. Responsibilities include:

- Clarifying meeting etiquette & use of chat beforehand, if necessary
- Preparing & following a clear meeting agenda that all attendees have access to
- Taking (or delegating) meeting notes that are sent out upon completion of meeting
- Introducing speakers, agenda topics, etc

Technological Responsibilities:

- Setting up the meeting space and ensuring attendees can login
- Muting other attendees when necessary
- Transferring screen sharing permissions to other presenters, when necessary
- If possible, having a tech-savvy back-up person in case of unforeseen difficulties

## (Short) Sample Meeting Agenda

Host greets attendees

Host confirms that all attendees have received and understand the meeting agenda

Host runs through meeting agenda topic by topic

- Host introduces each attendee to speak when it is his or her turn to contribute to the agenda
- Host asks if anyone has questions or concerns before moving to next agenda item
- If questions or concerns are outside scope of meeting, Host makes note to take topic offline and set up separate meeting/follow-up



### Keep that Human Connection

If you have the time, plan a few minutes of small talk into the agenda for the beginning of the meeting. The Host can ask each attendee to speak in turn so attendees get a chance to connect.



## Top Video Collaboration Tools

Choosing video collaboration over phone calls gets you seen, and heard, when working remotely. It's estimated that 4% multitask on video calls vs. 57% on phone calls.<sup>1</sup>



### Microsoft Teams

Microsoft Teams is the hub for team collaboration in Office 365 that integrates the people, content, and tools your team needs to be more engaged and effective.

[Remork Work With MS Teams](#)

### Best For:

- Internal and External chat + video collaboration
- Chat and Video Conferences up to 250 people

Additionally, MS Teams seamlessly integrates with all other Microsoft products



### Cisco Webex

Cisco Webex is a leading enterprise solution for video conferencing, online meetings, screen share, and webinars.

[Remote Work With Cisco Webex](#)

### Best For:

- Internal collaboration needs
- Remote meetings with medium-sized groups of participants (up to 200)



### Zoom

Zoom is a leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

[Remote Work With Zoom](#)

### Best For:

- Internal and External Video Conferencing

**Important note:** Zoom is a less mature platform than MS Teams or Cisco Webex, resulting in a number of security concerns and vulnerabilities. centrexIT advises against deploying Zoom over these more mature and secure offerings.



## How to Contact Us

No matter where you are in your business journey, our team can help you.



**619.651.8700**



[centrexIT.com/contact](http://centrexIT.com/contact)



### References

1. [The Me in Team: Drawing on the strengths of the individual to unleash the power of teams](#)
2. [The Pros and Cons of Working from Home](#)
3. [Microsoft: Using multi-factor authentication blocks 99.9% of account hacks](#)
4. [Pax8: The Official Wingman Guide to Remote Work](#)
5. [How to Work From Home: 20 Tips From People Who Do It Successfully](#)

 Taking Care of Business. That's **IT**.

centrexIT.com | 619.651.8700 | 3131 Camino Del Rio N Suite 1400, San Diego, CA 92108