Trillian

The ultimate communication security policy

CONTENTS

Introduction 3

What is a communication security policy? 4

The benefits 4

Start with a data risk assessment 5

Things to include in your communication security policy 6

What is on premises (or on-prem)? 9

About Cerulean 18

Introduction

Remote working is on the rise, and COVID-19 has opened up a new realm of data security issues.

Employees communicate internally and with third parties on a daily basis. With 49 percent of data breaches caused by human error, it's important to have a communication security policy in place to keep your data safe.

Creating any new company policy can be intimidating at first, but we've created editable checklists to steer you in the right direction.

What is a communication security policy?

A communication security policy is used to ensure the protection of information in your company networks and any supporting information processing facilities. It provides your team with communication security rules and standards to follow.

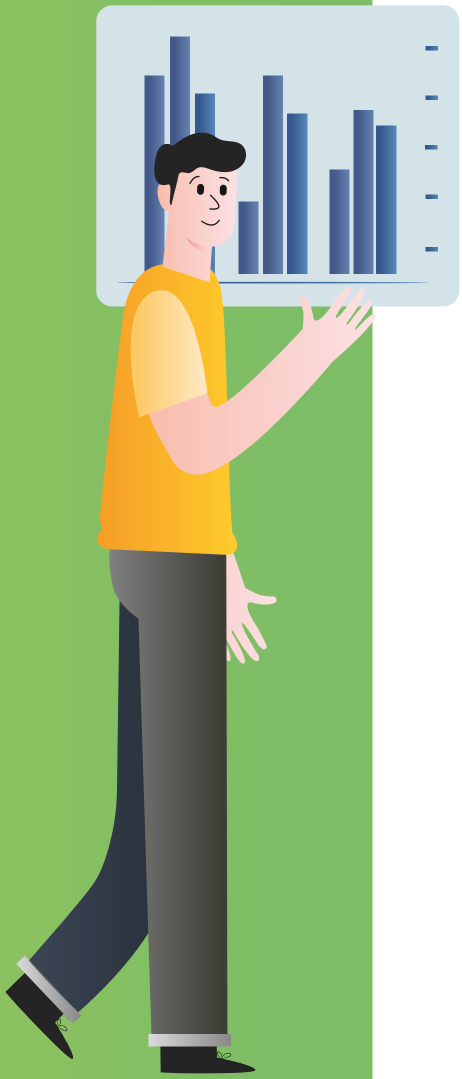
The benefits

The need to monitor employees both at home and in the workplace can make it challenging to create a secure business environment. Proactively setting rules and standards is a great way to ensure your company data is secure.

Creating a communication security policy:

- Minimizes the risk of data leaks or loss
- Sets guidelines and best practices
- Ensures compliance with industry-specific regulations
- Forewarns employees of the importance and standards around communication security
- Promotes a proactive stance for your organization if legal issues arise
- Protects your organization from malicious external and internal users

Now, let's get stuck into building your communication policy.

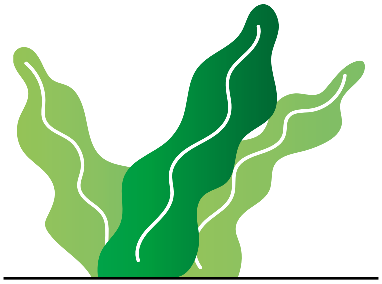


Start with a data risk assessment

Complete regular risk assessments to identify any potential threats to your organization's data. This will allow you to identify and review any obvious compromises – everything from an online data breach to more physical threats such as power cuts.

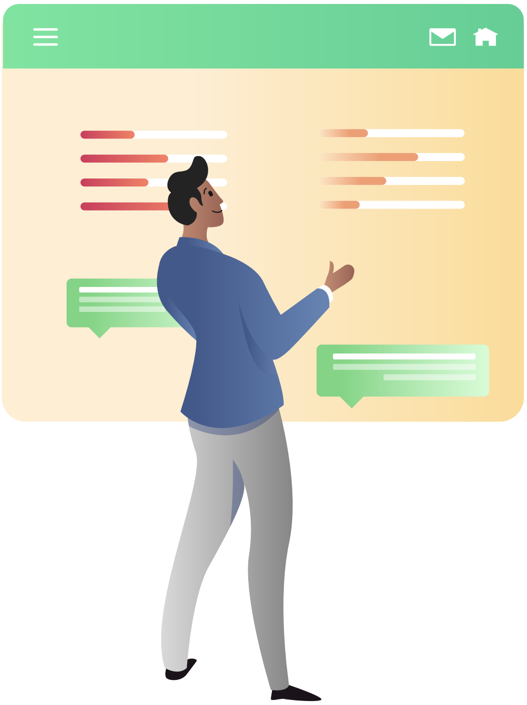
Regular risk assessments will also help you to manage your company data. During the assessment, explore your data retention methods. This will allow you to organise and clean up your data sets by deleting outdated information as well as backing up and securing anything that needs to be stored.

Data security incidents cost global businesses up to $3.86M a year on average. Prioritize these actions to reduce the risk of an expensive breach.



Things to include in your communication security policy

Where does your data live? And how do you control access to it? Answering these questions will help you discover the areas that need to be addressed in your policy. Get input from your employees and other key stakeholders. These are the people that will be affected by your decisions, after all.



Cloud vs on-premises

Let's take a look at where you store your communication data. Your business has a choice between on-premises or cloud solutions.

Lately, the cloud has become very popular. Despite this, on-premises implementations still have a vital role – especially within heavily-regulated industries:

Healthcare must follow things like the Health Insurance Portability and Accountability Act (HIPAA)

Educational institutions are subject to the Family Educational Rights and Privacy Act (FERPA)

Businesses handling credit card payments have to follow the Payment Card Industry Data Security Standard (PCI DSS)

Organizations subject to these standards often need to know exactly how their data is secured, and be able to prove it with documentation.

Security in the cloud

Cloud solutions mean your servers exist offsite. By paying a monthly fee, your business is able to store its data remotely. The cloud services provider takes care of security, maintenance, backups, software updates, power, and HVAC. Your company then relies on the internet to access its IT systems.

Before choosing a cloud solution, it's vital to learn about your provider's security protocols. Is the data center protected from intruders? Is software kept up-to-date with the latest security fixes? What measures are in place to protect against cybercriminals and disaster situations? Quality cloud providers will have watertight procedures and robust security teams.

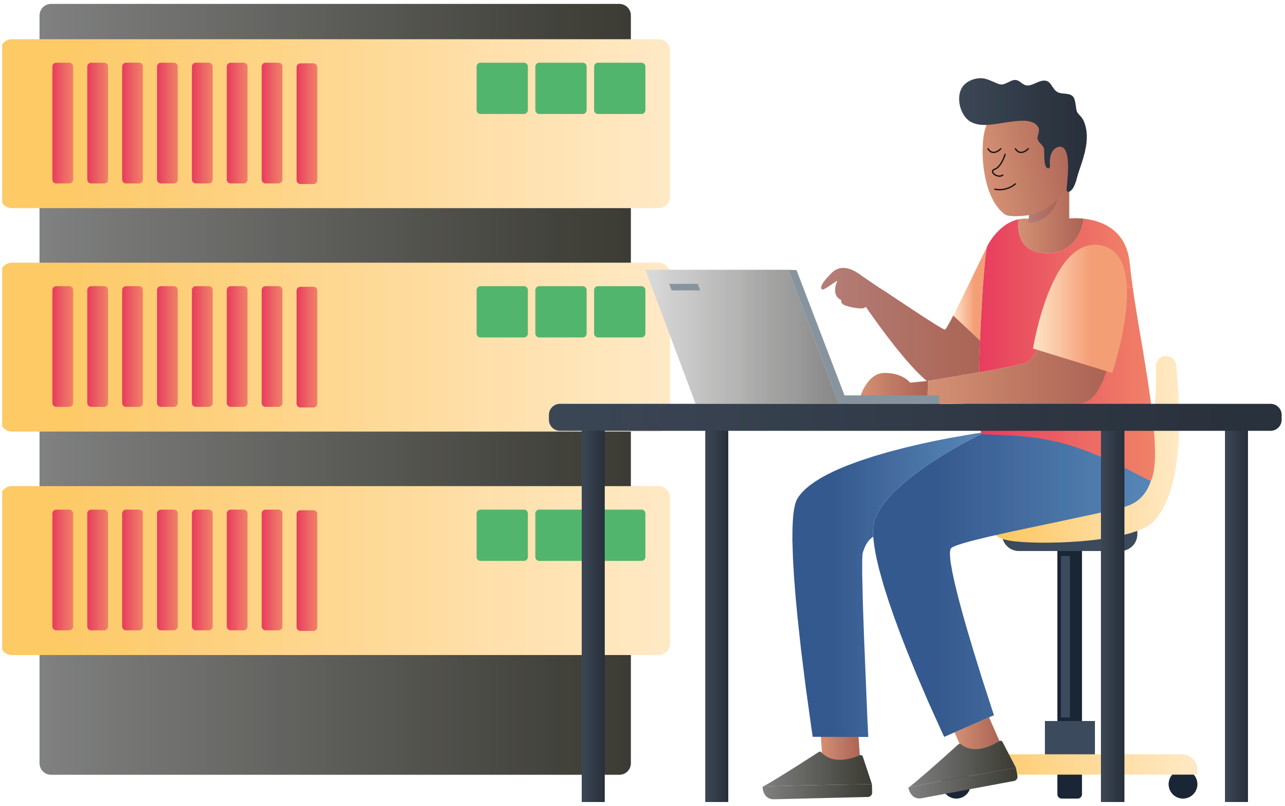
Cloud security checklist

Task	Assigned to	Due date	Status	Notes
Research multiple cloud providers				
Compare providers' security measures				
Decide on cloud service provider				
Add your own				
Add your own				
Add your own				

What is on premises (or on-prem)?

With ‘on-prem’, all hardware and software reside in-house. Your business will buy and maintain its own servers. To maintain security, Your IT team must keep your servers up-to-date with the latest software updates and perform regular backups. As your company expands, you might need to get new hardware to meet capacity demands.

A company running its own on-premises servers retains more complete control over network security. Because you are responsible for updates and maintenance, however, costs can add up quickly.



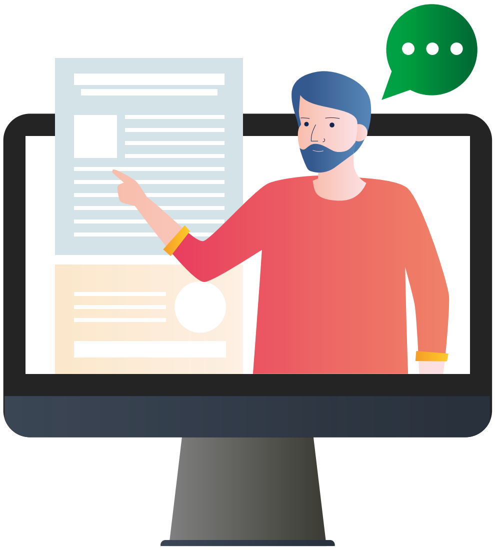
On-prem security checklist

Task	Assigned to	Due date	Status	Notes
Employ and install physical security measures				
Set up network elements and architecture				
Assign ownership of operation and maintenance, e.g. Installing firewalls and antivirus software				
Add your own				
Add your own				
Add your own				

More and more cloud providers are beginning to offer services that are aligned with industry regulations. There are tools available that provide the best of both worlds. Trillian, for example, is a secure, HIPAA-compliant messaging platform that works across desktop and mobile devices – and can be hosted on-prem or in the cloud.

On-prem security checklist

You've got to train your troops – they're your first line of defense and your weakest link. Unfortunately, employees can be negligent when it comes to sharing information, protecting their passwords or enabling two-factor authentication. As a result, regular security training is crucial.



This training should include:

- Incident response
- Emerging security issues and trends in your industry
- Current threats, such as phishing, spear phishing, social engineering, mobile security and ransomware
- Data sharing practices and access controls
- Effective password creation
- Network usage (i.e. promoting caution when using public networks)

There's a lot to learn when it comes to communication security. So, to get started, have a look at products and services you already use and see if they have training videos available. You'll be surprised at the helpful resources you may find.

Employee awareness and training checklist

Task	Assigned to	Due date	Status	Notes
Create an online survey to review what staff know about communication security				
Source experts for staff training in lacking areas				
Schedule training				
Create a best practice guide				
Have employees retake survey post training				
Ensure new hires receive accurate and updated training				
Add your own				
Add your own				
Add your own				

Remember, training is an ongoing process. As technology evolves, machines (and humans) get smarter. More intelligence means more advanced threats and attacks, so keep your employees vigilant at all times. Which brings us to...

Identity and Access Management (IAM)

A foundational step when it comes to communication and data security comes with making use of simple features that are included in most of the tools your company implements. Things like automatic screen locking and pin access are commonly available on most devices.

Administrative controls give you strict governance over identity and access management (IAM), such as user permissions and authorizations. They help you to keep track of your workforce and grant tailored, secure employee access.

Having a strong a control policy is critical for communication security. You need to regularly review who has access to important systems for it to be a success.

In addition to more general access management, your business will also need an effective password protection plan.

Password protection

Using strong passwords may seem like the simplest thing to some. However, you will be surprised how laid back some people are. In 2019, 23.2 million people worldwide used the password '123456'.

To employ and sustain a secure password protection policy, it's worth considering password management tools like LastPass, 1Password and Zoho Vault.

Multi-factor authentication (MFA)

It's not enough to depend on a single password to protect your business. With multi-factor authentication, you can add an extra layer of security to user sign-ins.

Setting this up will require your users to verify their identity via phone, text message or app notification before signing in. This makes it harder for an unauthorized user to hack into your business accounts.

IAM, password protection and MFA checklist

Task	Assigned to	Due date	Status	Notes
Review all employees' current access				
Remove admin access from those who no longer require it				
Set a monthly reminder to review access				
Employ and sustain a password protection policy				
Activate multi-factor authentication				
Add your own				
Add your own				
Add your own				

We also recommend that your employees only use regularly updated, company owned or provisioned 'Bring Your Own Device' (BYOD) devices. Ideally, you shouldn't allow any employee to work on unprotected devices.

BYOD security

Bring your own device (BYOD) refers to your employees using personal devices to connect to organizational networks and access work-related systems. Devices include smartphones, personal computers, laptops and tablets.

You can choose to include BYOD in your policy or have a strict 'no BYOD' policy. If you choose not to include a BYOD section in your policy, then you will have to supply employees with secure business only devices.

This section of your policy will cover:

- Acceptable use: what applications are employees permitted to access from their personal devices?
- The minimum required security controls for devices
- Company-provided components, such as SSL certificates for device authentication
- Company rights for altering the device, such as remote wiping for lost or stolen devices

BYOD security checklist

Task	Assigned to	Due date	Status	Notes
BYOD or ban BYOD?	Combined executive decision	October 21	Company meeting discussion	
Get input from key stakeholders				
Create a BYOD employee survey				
Process results of employee survey				
Determine devices allowed				
Decide rules around usage				
Provide devices OR install security controls/ measures on devices (employee or own)				
Add your own				
Add your own				
Add your own				

Communication security policies require continuous effort. They should be an ongoing feature of your company's security plans. Make sure you place defined importance on creating policies that'll keep your partners, clients and employees safe.

We've created this guide to get steer you in the right direction, and to help you identify areas in your internal and external communications that may need improvement. If you're still stuck in a rut, we're always here to help. If you have any questions – or would like to hear more about how our IM product Trillian can improve your communication security – feel free to contact us.

About Cerulean

Cerulean studios was founded in 2000, the same year Trillian started its long journey as an interoperable instant messaging client. After nearly 20 years in business, we can no longer convincingly call ourselves a startup but it certainly still feels that way! Our primary focus is on building services to help consumers and businesses alike leverage secure instant messaging to stay in touch and improve workplace collaboration. We believe that the internet would be a better place if instant messaging networks would play nice with each other and will continue doing our part to make this a reality.