

ALYSSA PUGH

How to Write a Policy



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.

Unauthorized release of this information is prohibited.

Original material is copyright © 2022 Tandem.



2



Alyssa Pugh

CISM, SECURITY+
TANDEM GRC CONTENT MANAGER



3

Agenda

HERE'S THE PLAN

- Policy Theory
- Policy Practice
 - Choose a Topic
 - Research
 - Draft Policy Sections
 - Get it Approved
- Questions & Answers



Policy

NAME

POLICY STATEMENT

COMMENTARY

IMPLEMENTATION

KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022



4



Policy Theory

WHAT'S IN A POLICY?

5

TANDEM POLICIES DOCUMENT INTRODUCTION

“Policies are a series of statements, rules, and assertions which define the organization’s governance structure.”



6

How Does it Do That?

1

Expected Behavior

(how you act)

2

Required Actions

(what you do)

3

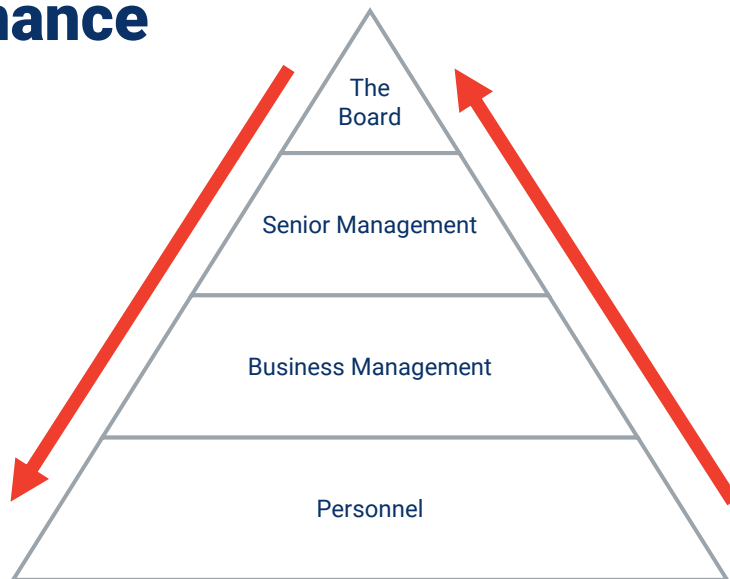
Prohibited Activities

(what you do not do)



7

Governance



8

<h1>Policy Sections</h1>	
	1 Name
Policy Statement	2
	3 Commentary
Implementation	4
	5 Related Policies
Responsibility	6
	7 Review Items



9

Policy

NAME

POLICY STATEMENT

COMMENTARY

IMPLEMENTATION

A brief title.

A summary.

This is the policy.

The context.

Justify and define.





10

IMPLEMENTATION

How you do the policy. Standards or procedures.

1 | KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022

11

RELATED POLICIES

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.


Topics related to this policy.

RESPONSIBILITY

Who makes it all happen.

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?
<input type="text"/>	<input type="text"/>	<input type="text"/>



12

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?	
			Prove the policy works.

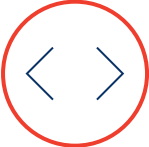


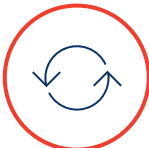


2 | KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022




13

What NOT to Do

IT'S A LONG LIST... BUT HERE'S SIX.

- 
Too Broad
- 
Too Specific
- 
Missing Key Words
- 
Duplicate Content
- 
Impossibly Formatted
- 
Not Followed



14

TAKEAWAY

**Policies are your friends.
Help them help you.**



15



Policy Practice

TIME TO ROLL UP YOUR SLEEVES

16

Disclaimers

A FEW MORE THINGS

Get up and stretch sometimes.

Writing a policy can cause muscle and brain cramps if not managed appropriately.

Do not throw your controller at the screen.

I borrowed this from Nintendo, but it is a good rule to live by, especially when writing policies.

You might not need the policy we write today.

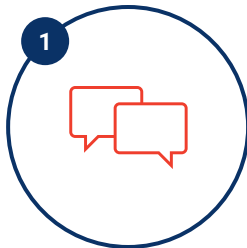
Your organization's size, complexity, systems, and processes will determine what policies you need.



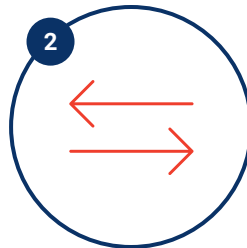
17

Pick a Policy

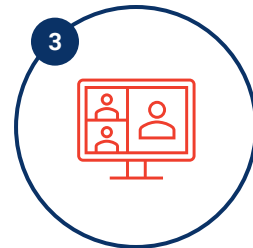
CHOOSE YOUR OWN ADVENTURE!



Instant Messaging
Policy



File Exchange
Policy



Video Conferencing
Policy

Cloud Computing Policy



18



Video Conferencing Policy

YOU CHOSE... WISELY.

19

Examples



Zoom



Google Meet



Webex



Teams

A video conferencing application allows users to host, join, and record virtual meetings, including audio, video, and text communications.



20

Policy

NAME *A brief title.*


POLICY STATEMENT

*A summary.
This is the policy.*

COMMENTARY

*The context.
Justify and define.*

IMPLEMENTATION



21

Policy

NAME *A brief title.*


POLICY STATEMENT

*A summary.
This is the policy.*

COMMENTARY

*The context.
Justify and define.*

IMPLEMENTATION



22

Policy

NAME Video Conferencing

A brief title.

POLICY STATEMENT

Use only approved video conferencing applications for virtual meetings in which organization and/or customer/member data may be discussed.

A summary.
This is the policy.

COMMENTARY

1. Define "Video Conferencing."
2. Describe the benefits and risks.
3. Explain how the policy helps.

The context.
Justify and define.

IMPLEMENTATION



23

IMPLEMENTATION



How you do the policy, standards or procedures.

¹ KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022



24

What Should You Do?

LOOK INSIDE YOUR HEART... AND THESE DOCUMENTS.

- FFIEC [IT Examination Handbook](#) (“IT Booklets”)
- FFIEC [Cybersecurity Assessment Tool](#) (CAT)
- NIST [Cybersecurity Framework](#) (CSF)
- NIST [SP800-53 Controls](#)
- CIS [Controls](#) (v8.0)
- CISA [Tips](#) and [Alerts](#)
- Agency IT Examination Procedures (e.g., FDIC [InTREx Program](#))
- Agency Guidance (e.g., FDIC FILs; FRB SR Letters; NCUA SLs; OCC Bulletins)



25

Web Search

SECRETS OF A POLICY WRITER

[Topic] site:".gov"



Video Conferencing Guidance site:".gov"



26

video conferencing site:".gov" 🔍

[🔍 All](#) [🖼️ Images](#) [▶ Videos](#) [📰 News](#) [📍 Maps](#) [🛒 Shopping](#) [Settings ▾](#)

All regions ▾ Safe search: moderate ▾ Any time ▾

Showing results from: ".gov" All Results

freeconferencecall.com | Report Ad

Like Zoom But Free - Official Site AD

Host Unlimited Free Conference Calls With Free Recording. Sign Up In Seconds! We have an average rating of 4.5 stars on TrustPilot (spoiler: Zoom's is only 1.8 stars).
Up To 1,000 Callers - Now With HD Quality - 24/7 Customer Support
Service catalog: Video Calling, Conference Calling, Phone Calling

spotme.com | Report Ad


Deliver an Amazing Experience - SpotMe Virtual Event Platform AD

All the features and integrations you need to drive engagement and start conversations. Produce high quality, live or on-demand virtual conferences and events with SpotMe
Service catalog: Virtual Events & Webinars, Easy-to-Use Platform

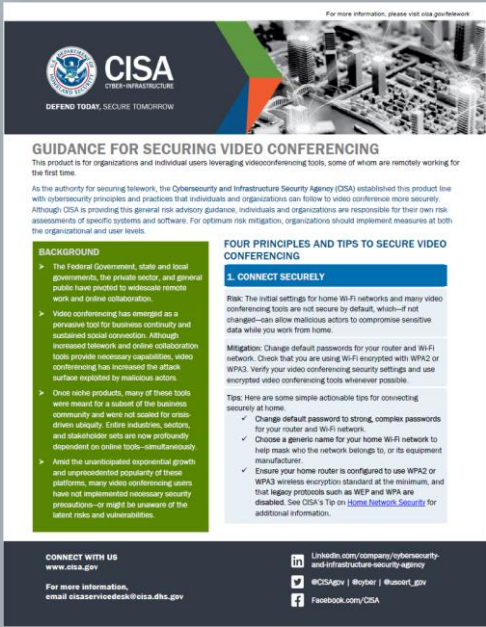
📄 https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securin...

📄 **Guidance for Securing Video Conferencing - CISA**

Risk: Outdated or unpatched video conference applications can expose security flaws for hackers to exploit, resulting in a disruption of meeting privacy and potential loss of information.
Mitigation: Ensure all video conferencing tools, on desktops and mobile devices, are updated to the latest versions.



27



CISA
DEFEND TODAY. SECURE TOMORROW

GUIDANCE FOR SECURING VIDEO CONFERENCING

This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing the network, the Cybersecurity and Infrastructure Security Agency (CISA) established this product line with cybersecurity principles and practices that individuals and organizations can follow to video conference more securely. Although CISA is providing this general risk advisory guidance, individuals and organizations are responsible for their own risk assessments of specific systems and software. For optimum risk mitigation, organizations should implement measures at both the organizational and user levels.

BACKGROUND

- The federal Government, state and local governments, the private sector, and general public have profited to widespread remote work and online collaboration.
- Video conferencing has emerged as a pervasive tool for business continuity and sustained social connection. Although increased network and device collaboration tools provide necessary capabilities, video conferencing has increased the attack surface required by malicious actors.
- On-line products, many of those tools were meant for a subset of the business community and were not scaled for crisis-driven security. Entire industries, sectors, and stakeholder sets are now profoundly dependent on online tools—simultaneously.
- Amid the unprecedented exponential growth and unprecedented popularity of these platforms, many video conferencing users have not implemented necessary security precautions—or might be unaware of the latest risks and vulnerabilities.

FOUR PRINCIPLES AND TIPS TO SECURE VIDEO CONFERENCING

1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home.

Mitigation: Change default passwords for your router and Wi-Fi network. Check that you are using Wi-Fi encrypted with WPA2 or WPA3. Verify your video conferencing security settings and use encrypted video conferencing tools whenever possible.

Tips: Here are some simple actionable tips for connecting securely at home.

- Change default password to strong, complex passwords for your router and Wi-Fi networks.
- Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
- Ensure your home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum, and that legacy protocols such as WEP and WPA are disabled. See CISA's Tip on [Home Network Security](#) for additional information.


CONNECT WITH US
www.cisa.gov

For more information, email cisasevice@csa.dhs.gov

[LinkedIn.com/company/cybersecurity-and-infrastructure-security-agency](https://www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency)
[@ICSAGov](https://twitter.com/ICSAGov) | [YouTube](https://www.youtube.com/channel/UC4w0rt_gjv)
[Facebook.com/CISA](https://www.facebook.com/CISA)

CISA
Guidance for Securing Video Conferencing

[Read the Guidance](#)



28

IMPLEMENTATION

1. Determine data to be stored, processed, or transmitted by video conferencing application.
2. Select a reputable service provider and perform adequate due diligence.
3. Block unauthorized video conferencing applications.
4. Train staff and include in acceptable use.
5. Follow security best practices, as defined by other policies, based on sensitivity of data.

How you do the policy. Standards or procedures.

1 | KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022



RELATED POLICIES

1. Access Control
2. Data Backup
3. Data Retention & Destruction
4. Encryption
5. IT Asset Management
6. System Hardening
7. Vendor Management

Topics related to this policy.

RESPONSIBILITY

Who makes it all happen.

REVIEW ITEMS

WHO?

WHAT?

HOW OFTEN?



RELATED POLICIES

- 1. Access Control
- 2. Data Backup
- 3. Data Retention & Destruction
- 4. Encryption
- 5. IT Asset Management
- 6. System Hardening
- 7. Vendor Management


RESPONSIBILITY

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?
<input type="text"/>	<input type="text"/>	<input type="text"/>

Topics related to this policy.

Who makes it all happen.





31

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?
Audit Committee	Review the use of video conferencing apps.	Annually
Vendor Management	Review updated service provider due diligence.	Annually
Security Committee	Review network logs to verify acceptable use.	Annually
Security Committee	Review security awareness training results and AUPs.	Annually

Prove the policy works.

2 | KEYS Session: How to Write a Policy
Tandem, LLC Copyright © 2022

32

Get it Approved!

Policy


NAME *A brief title.*


POLICY STATEMENT

"IT" → *A summary. This is the policy.*

COMMENTARY

Context of the policy (e.g. justification)





33

Policy

NAME *A brief title.*

POLICY STATEMENT

A summary. This is the policy.


COMMENTARY


The context. Justify and define.

IMPLEMENTATION

How you do the policy. Standards or procedures.

1 | KEYS Guides: How to Write a Policy Tandem, LLC Copyright © 2022





34

TAKEAWAY

The best policies are the ones which everyone can understand and follow.



35



36



KEYS
CONFERENCE

DON'T FORGET!

Fill out the survey to get your sticker!

37



THANKS FOR JOINING!

How to Write a Policy

Alyssa Pugh
CISM, SECURITY+
TANDEM GRC CONTENT MANAGER

38

Upcoming Sessions

TANDEM

Creating an Effective Incident Response Plan

Lindsey McReynolds, Tandem

RISK & COMPLIANCE

CoNetrix Security Auditors: A Panel Discussion

Mark Faske, Bret Mills, Mark Riff, & Ty Purcell, CoNetrix Security

CYBERSECURITY

Understanding the Value of Your SIEM and SOC

Mike Richline, CoNetrix Technology

