ALYSSA PUGH

How to Write a Policy

KEYS CONFERENCE

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.

KEYS CONFERENCE

2

Alyssa Pugh

CISM, SECURITY+
TANDEM GRC CONTENT MANAGER

KEYS CONFERENCE

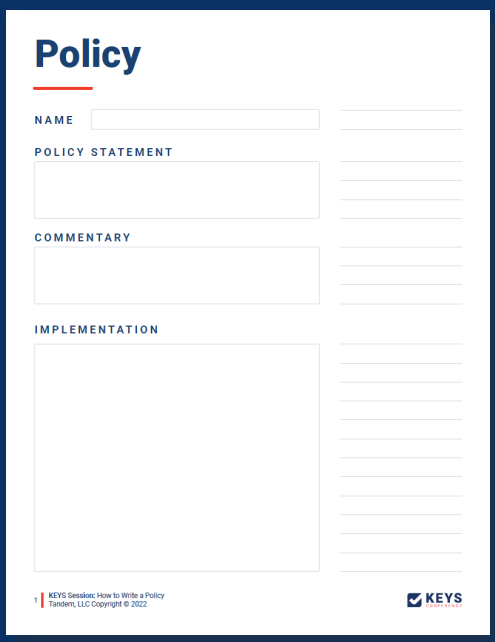
3

Agenda

HERE'S THE PLAN

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

KEYS CONFERENCE



4

KEYS CONFERENCE

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."

KEYS CONFERENCE

6

How Does it Do That?

1

Expected Behavior

(how you act)

2

Required Actions

(what you do)

3

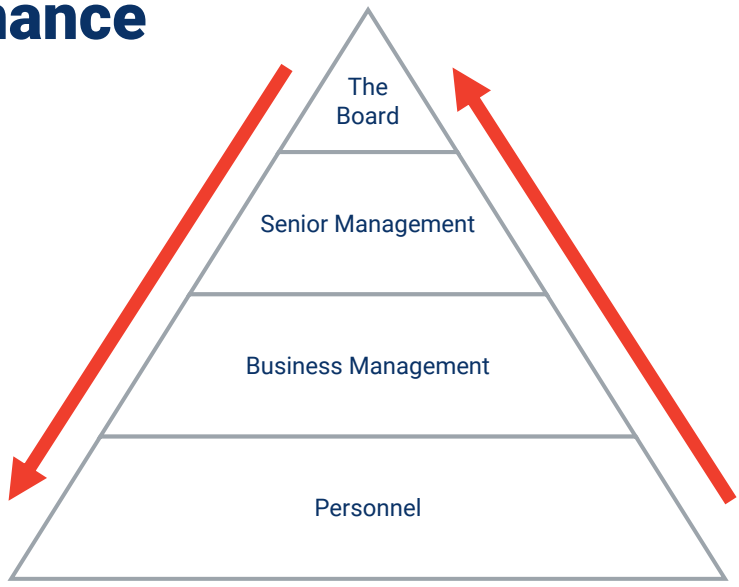
Prohibited Activities

(what you do not do)

KEYS CONFERENCE

7

Governance



KEYS CONFERENCE

8

Policy Sections

1. Name
2. Policy Statement
3. Commentary
4. Implementation
5. Related Policies
6. Responsibility
7. Review Items

KEYS CONFERENCE

9

Policy

NAME

A brief title.

POLICY STATEMENT

A summary.
This is the policy.

COMMENTARY

The context.
Justify and define.

IMPLEMENTATION

KEYS CONFERENCE

10

IMPLEMENTATION

How you do the policy. Standards or procedures.

KEYS CONFERENCE

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?

KEYS CONFERENCE

12

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?

Prove the policy works.

KEYS CONFERENCE

KEYS CONFERENCE

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

KEYS CONFERENCE

14

TAKEAWAY

Policies are your friends. Help them help you.

KEYS CONFERENCE

15

KEYS CONFERENCE

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.

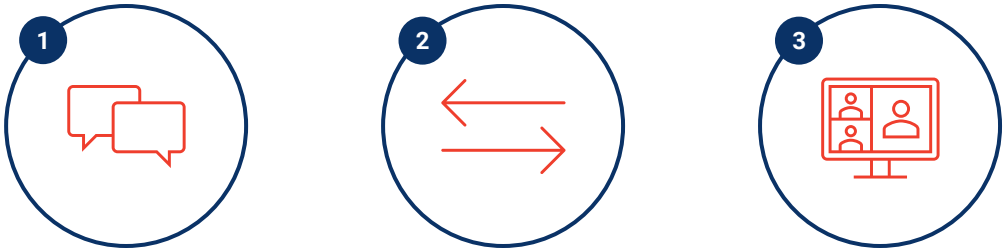
You might not need the policy we write today.
Your organization's size, complexity, systems, and processes will determine what policies you need.

KEYS CONFERENCE

17

Pick a Policy

CHOOSE YOUR OWN ADVENTURE!



Instant Messaging Policy

File Exchange Policy

Video Conferencing Policy

Cloud Computing Policy

KEYS CONFERENCE

18

KEYS CONFERENCE

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.

KEYS CONFERENCE

20

Policy

NAME Video Conferencing

A brief title.

POLICY STATEMENT

A summary.
This is the policy.

COMMENTARY

The context.
Justify and define.

IMPLEMENTATION

KEYS CONFERENCE

21

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

The context.
Justify and define.

IMPLEMENTATION

KEYS CONFERENCE

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

KEYS CONFERENCE

23

IMPLEMENTATION

How you do the policy. Standards or procedures.

KEYS CONFERENCE

KEYS CONFERENCE

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)

KEYS CONFERENCE

25

Web Search

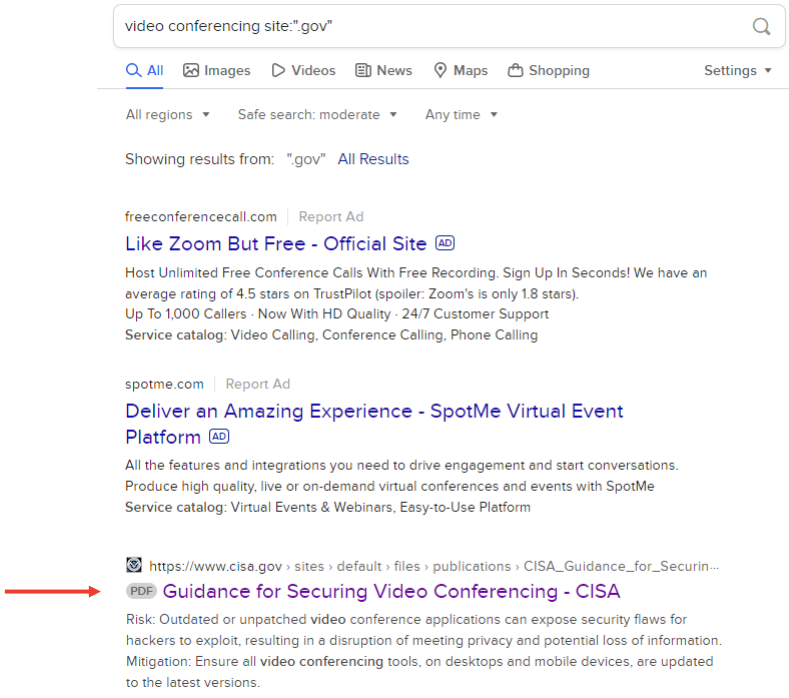
SECRETS OF A POLICY WRITER

[Topic] site:“.gov”

Video Conferencing Guidance site:“.gov”

KEYS CONFERENCE

26



27

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.

KEYS CONFERENCE

29

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?

KEYS CONFERENCE

30

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 *[[Name]]*

Who makes it all happen.

REVIEW ITEMS

WHO?	WHAT?	HOW OFTEN?

KEYS CONFERENCE

31

REVIEW ITEMS

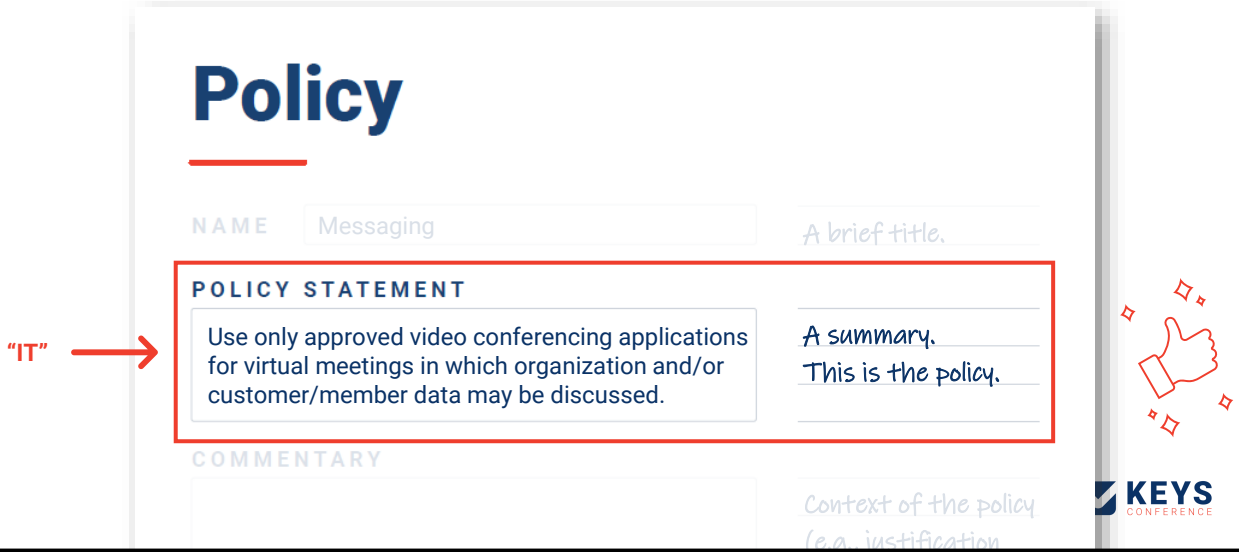
WHO?	WHAT?	HOW OFTEN?
Audit Committee	Review the use of video conferencing apps.	Annually
Vendor Management	Review updated service provider due diligence.	Annually
Security Committee	Review network logs to verify acceptable use.	Annually
Security Committee	Review security awareness training results and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

Prove the policy works.

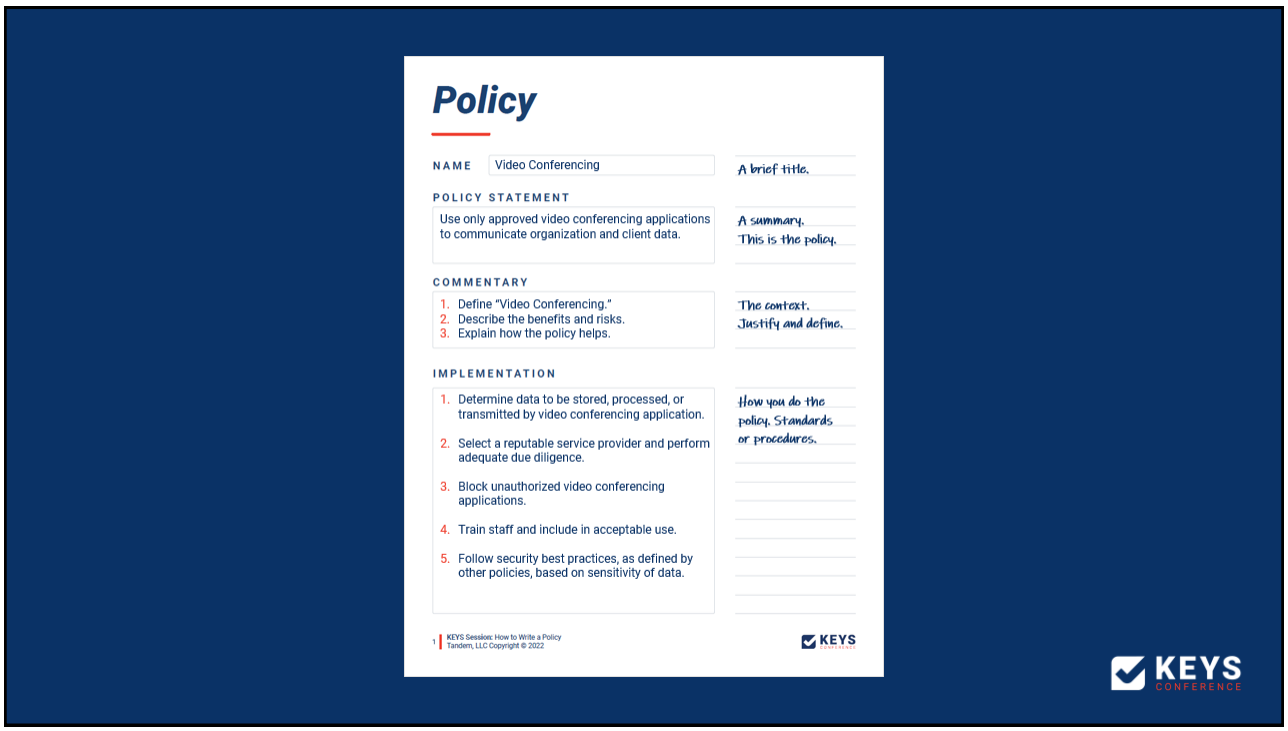
KEYS CONFERENCE

32

Get it Approved!



33



34

TAKEAWAY

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

KEYS CONFERENCE

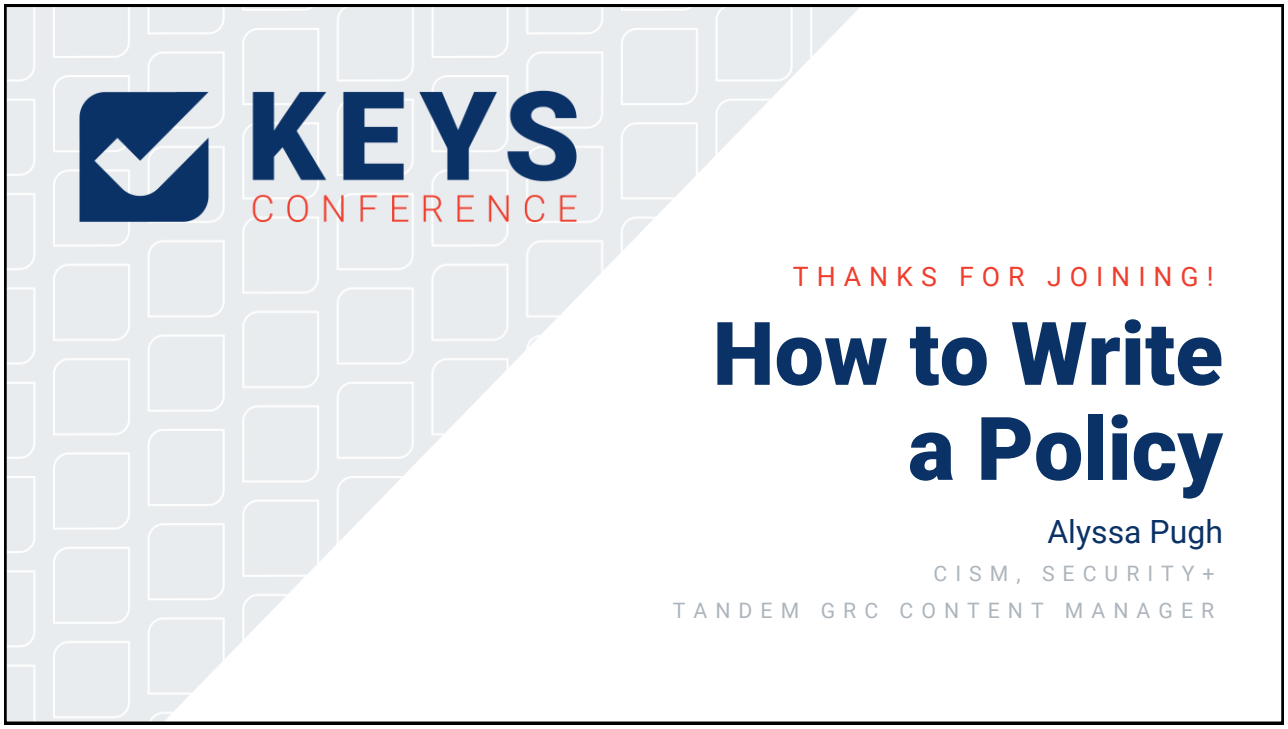
35

KEYS CONFERENCE

36


KEYS
CONFERENCE
DON'T FORGET!
Fill out the survey to get your sticker!

37


KEYS
CONFERENCE
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

KEYS CONFERENCE

39