Writing Policies That Aren’t Miserable for Everyone Involved

Nick Leghorn
Director, Application Security
The New York Times

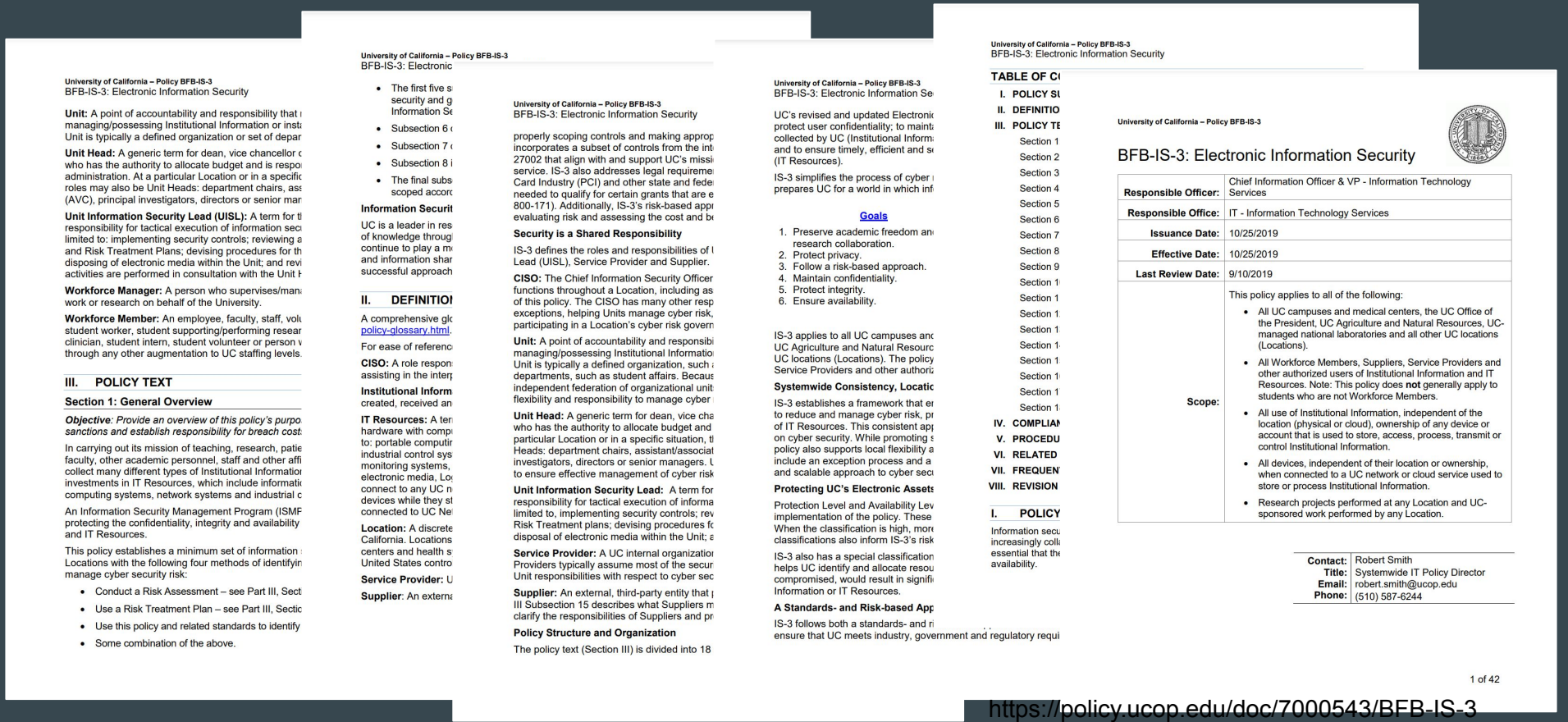
Disclaimer:

None of the information provided in this presentation is derived from, related to, or includes any information about the internal operations of the New York Times.

I cannot guarantee that the format and concept described in this presentation will satisfy your specific auditors or regulators. Please ensure that you consult your specific stakeholders before implementation.

How Many People Have Actually Read Their Corporate Security Policies?

Typical Information Security Policy



University of California – Policy BFB-IS-3
BFB-IS-3: Electronic Information Security

Unit: A point of accountability and responsibility that
managing/possessing Institutional Information or insta
Unit is typically a defined organization or set of depar

Unit Head: A generic term for dean, vice chancellor
who has the authority to allocate budget and is respo
administration. At a particular Location or in a specific
roles may also be Unit Heads: department chairs, ass
(AVC), principal investigators, directors or senior mar

Unit Information Security Lead (UISL): A term for t
responsibility for tactical execution of information sec
limited to: implementing security controls; reviewing a
and Risk Treatment Plans; devising procedures for th
disposing of electronic media within the Unit; and revi
activities are performed in consultation with the Unit

Workforce Manager: A person who supervises/mana
work or research on behalf of the University.

Workforce Member: An employee, faculty, staff, volu
student worker, student supporting/performing researc
clinician, student intern, student volunteer or person
through any other augmentation to UC staffing levels.

III. POLICY TEXT

Section 1: General Overview

***Objective**: Provide an overview of this policy's purpo
sanctions and establish responsibility for breach cost*

In carrying out its mission of teaching, research, patie
faculty, other academic personnel, staff and other affi
collect many different types of Institutional Informatio
investments in IT Resources, which include informatic
computing systems, network systems and industrial c

An Information Security Management Program (ISMF
protecting the confidentiality, integrity and availability
and IT Resources.

This policy establishes a minimum set of information
Locations with the following four methods of identifyin
manage cyber security risk:

- Conduct a Risk Assessment – see Part III, Sect
- Use a Risk Treatment Plan – see Part III, Sectic
- Use this policy and related standards to identify
- Some combination of the above.

University of California – Policy BFB-IS-3
BFB-IS-3: Electronic

- The first five s
security and g
Information Se
- Subsection 6
- Subsection 7
- Subsection 8 i
- The final subs
scoped accor

Information Securit

UC is a leader in res
of knowledge throug
continue to play a m
and information shar
successful approach

II. DEFINITIO

A comprehensive gl
policy-glossary.html.

For ease of referenc

CISO: A role respon
assisting in the interp

Institutional Inform
created, received an

IT Resources: A ter
hardware with compu
to: portable computir
industrial control sys
monitoring systems,
electronic media, Lo
connect to any UC n
devices while they st
connected to UC Ne

Location: A discrete
California. Locations
centers and health s
United States contro

Service Provider: U

Supplier: An externa

University of California – Policy BFB-IS-3
BFB-IS-3: Electronic Information Security

properly scoping controls and making approp
incorporates a subset of controls from the int
27002 that align with and support UC's missi
service. IS-3 also addresses legal requireme
Card Industry (PCI) and other state and fede
needed to qualify for certain grants that are e
800-171). Additionally, IS-3's risk-based appr
evaluating risk and assessing the cost and b

Security is a Shared Responsibility

IS-3 defines the roles and responsibilities of
Lead (UISL), Service Provider and Supplier.

CISO: The Chief Information Security Officer
functions throughout a Location, including as
of this policy. The CISO has many other resp
exceptions, helping Units manage cyber risk,
participating in a Location's cyber risk govern

Unit: A point of accountability and responsibi
managing/possessing Institutional Informatio
Unit is typically a defined organization, such
departments, such as student affairs. Becaus
independent federation of organizational unit
flexibility and responsibility to manage cyber

Unit Head: A generic term for dean, vice cha
who has the authority to allocate budget and
particular Location or in a specific situation, t
Heads: department chairs, assistant/associat
investigators, directors or senior managers. U
to ensure effective management of cyber risk

Unit Information Security Lead: A term for
responsibility for tactical execution of informa
limited to, implementing security controls; rev
Risk Treatment plans; devising procedures fo
disposal of electronic media within the Unit; a

Service Provider: A UC internal organizatio
Providers typically assume most of the secur
Unit responsibilities with respect to cyber sec

Supplier: An external, third-party entity that
III Subsection 15 describes what Suppliers m
clarify the responsibilities of Suppliers and pr

Policy Structure and Organization

The policy text (Section III) is divided into 18

University of California – Policy BFB-IS-3
BFB-IS-3: Electronic Information Se

UC's revised and updated Electronic
protect user confidentiality; to maint
collected by UC (Institutional Inform
and to ensure timely, efficient and s
(IT Resources).

IS-3 simplifies the process of cyber
prepares UC for a world in which inf

Goals

1. Preserve academic freedom an
research collaboration.
2. Protect privacy.
3. Follow a risk-based approach.
4. Maintain confidentiality.
5. Protect integrity.
6. Ensure availability.

IS-3 applies to all UC campuses an
UC Agriculture and Natural Resourc
UC locations (Locations). The policy
Service Providers and other authori

Systemwide Consistency, Locatic

IS-3 establishes a framework that e
to reduce and manage cyber risk, p
of IT Resources. This consistent ap
on cyber security. While promoting
policy also supports local flexibility a
include an exception process and a
and scalable approach to cyber sec

Protecting UC's Electronic Assets

Protection Level and Availability Lev
implementation of the policy. These
When the classification is high, more
classifications also inform IS-3's risk

IS-3 also has a special classification
helps UC identify and allocate resou
compromised, would result in signifi
Information or IT Resources.

A Standards- and Risk-based App

IS-3 follows both a standards- and ri
ensure that UC meets industry, government and regulatory requi

University of California – Policy BFB-IS-3
BFB-IS-3: Electronic Information Security

TABLE OF C

I. POLICY SU
II. DEFINITIO
III. POLICY TE
Section 1
Section 2
Section 3
Section 4
Section 5
Section 6
Section 7
Section 8
Section 9
Section 1
Section 1
Section 1
Section 1
Section 1
Section 1
Section 1
Section 1
Section 1
IV. COMPLIAN
V. PROCEDU
VI. RELATED
VII. FREQUEN
VIII. REVISION

I. POLICY

Information secu
increasingly colli
essential that the
availability.

University of California – Policy BFB-IS-3

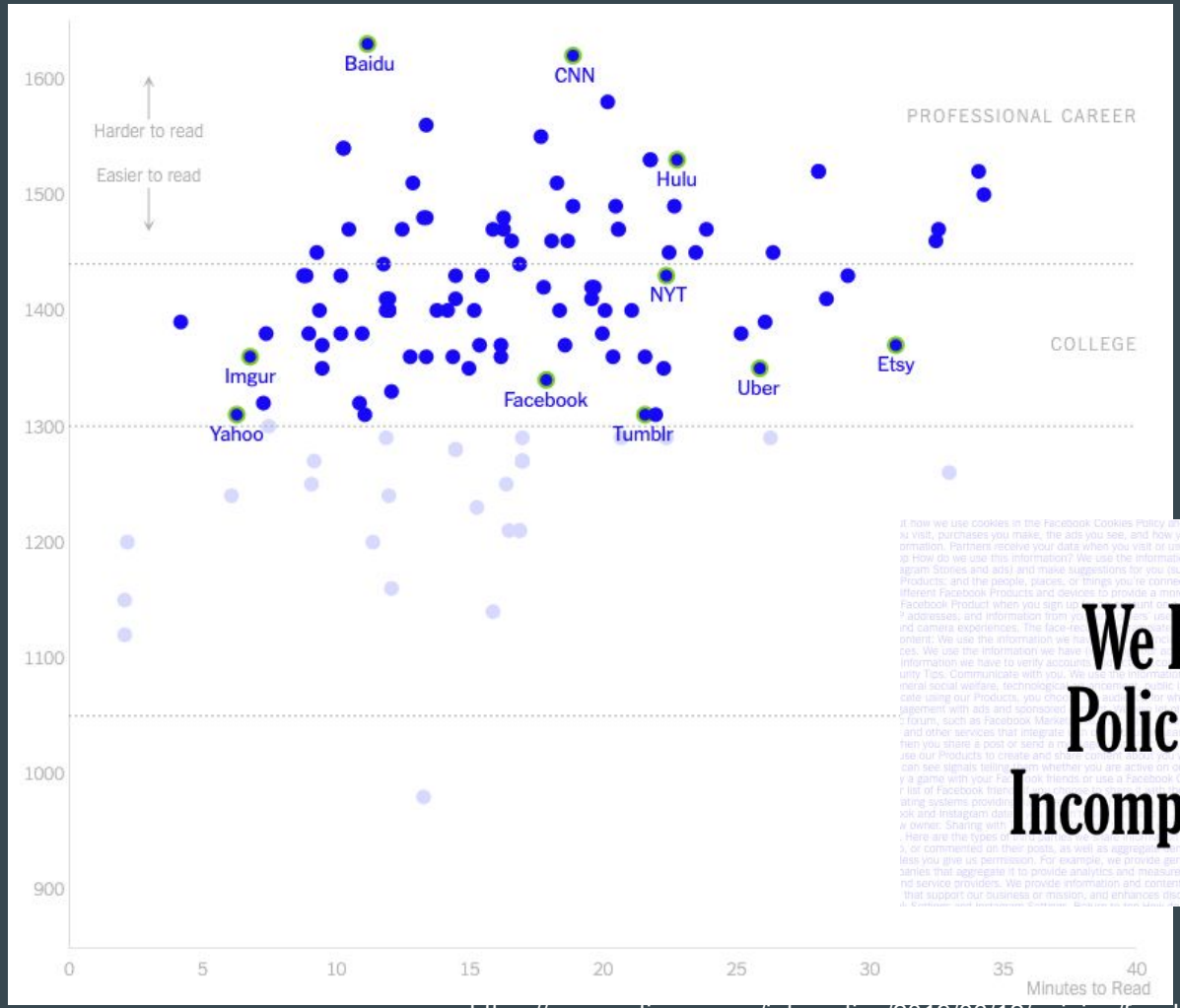
BFB-IS-3: Electronic Information Security

Responsible Officer:	Chief Information Officer & VP - Information Technology Services
Responsible Office:	IT - Information Technology Services
Issuance Date:	10/25/2019
Effective Date:	10/25/2019
Last Review Date:	9/10/2019
Scope:	This policy applies to all of the following: • All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories and all other UC locations (Locations). • All Workforce Members, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources. Note: This policy does **not** generally apply to students who are not Workforce Members. • All use of Institutional Information, independent of the location (physical or cloud), ownership of any device or account that is used to store, access, process, transmit or control Institutional Information. • All devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information. • Research projects performed at any Location and UC-sponsored work performed by any Location.

Contact:	Robert Smith
Title:	Systemwide IT Policy Director
Email:	robert.smith@ucop.edu
Phone:	(510) 587-6244

1 of 42

https://policy.ucop.edu/doc/7000543/BFB-IS-3



Opinion | THE PRIVACY PROJECT

We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

By Kevin Litman-Navarro

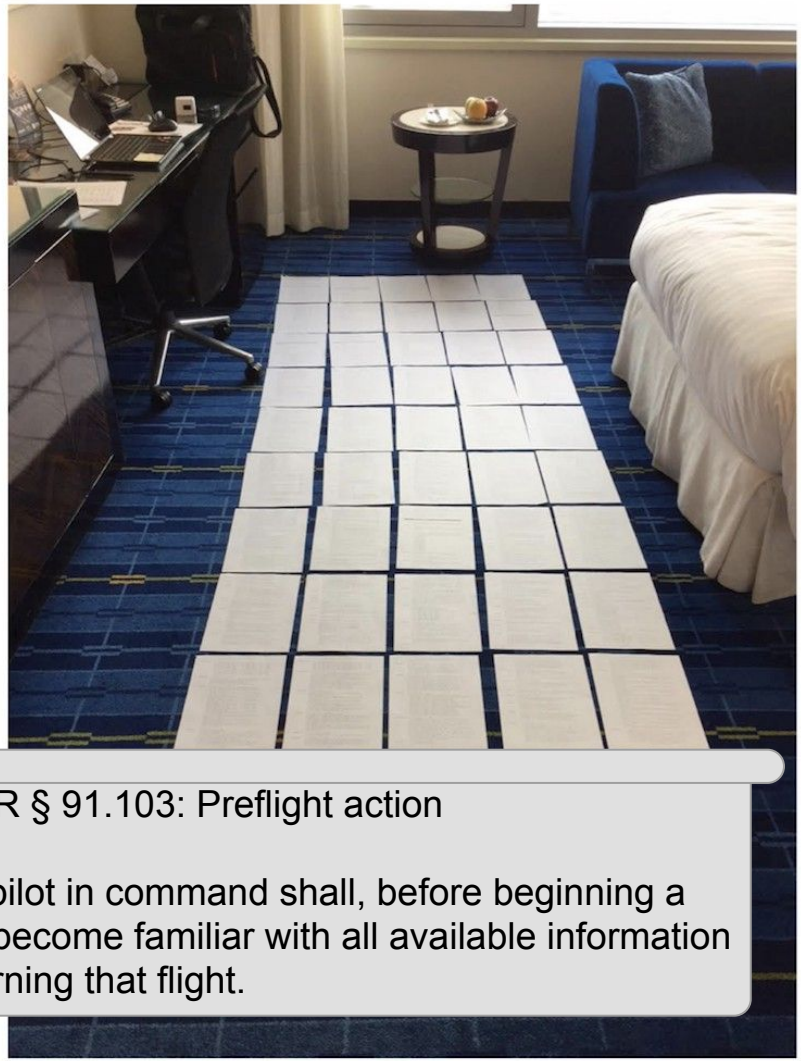
https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

Typical InfoSec Policy Drivers

- Legal obligations
  - Meeting requirements of specific laws and regulations
  - Reducing legal liability
- Compliance obligations
  - HIPAA / CCPA / GDPR / etc
  - SOC2 / PCI
  - 3rd Party Requirements
- HR Support
  - Providing rationale for terminations

Policies Reflect the Audience

This Problem Isn’t Unique to Policies



14 CFR § 91.103: Preflight action

Each pilot in command shall, before beginning a flight, become familiar with all available information concerning that flight.

Information Needs To Be Useful

BUSINESS

Allegiant defends emergency landing at closed airport

Allegiant is the dominant carrier operating out of St. Pete-Clearwater International Airport. [DOUGLAS R. CLIFFORD | Times]

By **Times Staff Writer**

Published Jul. 30, 2015

Allegiant Air defended itself on Thursday amid a Federal Aviation Administration investigation into an emergency landing one of the airline's jets made last week at a closed airport while running low on fuel.

News

NTSB finds pilot in 2011 crash did not request weather briefing

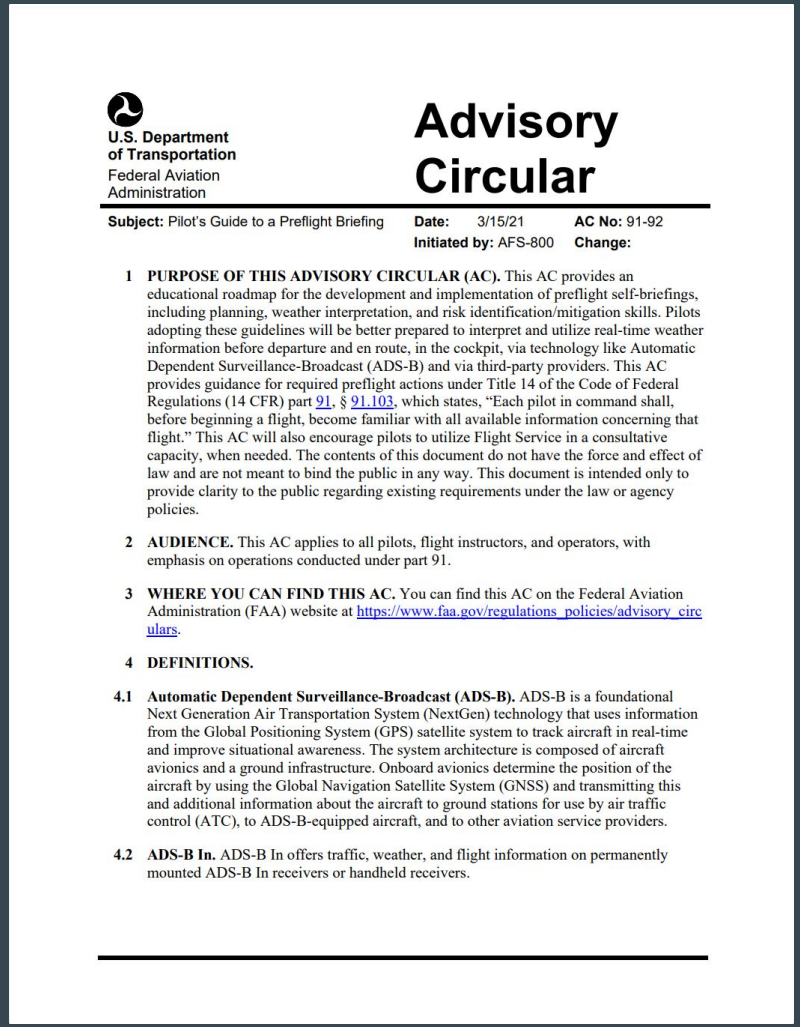
Updated: Mar. 30, 2019, 10:10 a.m. | Published: Jan. 26, 2013, 11:00 a.m.

Wreckage of the plane that crashed onto Interstate 287 in December 2011, killing all five people on board. The NTSB, in a new report, said the pilot appeared to have encountered severe icing conditions.

FAA AC 91-92

March 15, 2021

- Acknowledges that these pre-flight briefings are too complex to actually understand.
- Important details are hidden among a sea of unimportant garbage.
- FAA is working on finding ways to improve briefings.
- Recommends that pilots use other sources in the meantime.



U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: Pilot's Guide to a Preflight Briefing **Date:** 3/15/21 **AC No:** 91-92
Initiated by: AFS-800 **Change:**

1 **PURPOSE OF THIS ADVISORY CIRCULAR (AC).** This AC provides an educational roadmap for the development and implementation of preflight self-briefings, including planning, weather interpretation, and risk identification/mitigation skills. Pilots adopting these guidelines will be better prepared to interpret and utilize real-time weather information before departure and en route, in the cockpit, via technology like Automatic Dependent Surveillance-Broadcast (ADS-B) and via third-party providers. This AC provides guidance for required preflight actions under Title 14 of the Code of Federal Regulations (14 CFR) part 91, § 91.103, which states, "Each pilot in command shall, before beginning a flight, become familiar with all available information concerning that flight." This AC will also encourage pilots to utilize Flight Service in a consultative capacity, when needed. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

2 **AUDIENCE.** This AC applies to all pilots, flight instructors, and operators, with emphasis on operations conducted under part 91.

3 **WHERE YOU CAN FIND THIS AC.** You can find this AC on the Federal Aviation Administration (FAA) website at https://www.faa.gov/regulations_policies/advisory_circulars.

4 **DEFINITIONS.**

4.1 **Automatic Dependent Surveillance-Broadcast (ADS-B).** ADS-B is a foundational Next Generation Air Transportation System (NextGen) technology that uses information from the Global Positioning System (GPS) satellite system to track aircraft in real-time and improve situational awareness. The system architecture is composed of aircraft avionics and a ground infrastructure. Onboard avionics determine the position of the aircraft by using the Global Navigation Satellite System (GNSS) and transmitting this and additional information about the aircraft to ground stations for use by air traffic control (ATC), to ADS-B-equipped aircraft, and to other aviation service providers.

4.2 **ADS-B In.** ADS-B In offers traffic, weather, and flight information on permanently mounted ADS-B In receivers or handheld receivers.

Back to Basics:
Why Do Policies Exist?

Objective: Reduce Risk to the Business

We reduce risk to the business by establishing expectations for how employees make decisions.

We want employees to consistently follow a set of approved rules in their daily job.

Policies Should Be Crafted for **Employees**

Legal / Compliance / HR Are **Stakeholders**

Let’s Deconstruct Policies and Build Them Better

Policy Components

Scope and Applicability

Who needs to care about this policy

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve
References	What frameworks, laws, or other documents does this policy draw from for its components

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve
References	What frameworks, laws, or other documents does this policy draw from for its components
Policy Statement	Statement of intent from management for how employees or the business should behave

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve
References	What frameworks, laws, or other documents does this policy draw from for its components
Policy Statement	Statement of intent from management for how employees or the business should behave
Standards	Specific **implementation agnostic** requirements for how to achieve the objectives and policy statement

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve
References	What frameworks, laws, or other documents does this policy draw from for its components
Policy Statement	Statement of intent from management for how employees or the business should behave
Standards	Specific **implementation agnostic** requirements for how to achieve the objectives and policy statement
Guidelines	More detailed **implementation specific** guidance for how to achieve the requirements defined by the standards

Policy Components

Scope and Applicability	Who needs to care about this policy
Objectives	What does the policy hope to achieve
References	What frameworks, laws, or other documents does this policy draw from for its components
Policy Statement	Statement of intent from management for how employees or the business should behave
Standards	Specific **implementation agnostic** requirements for how to achieve the objectives and policy statement
Guidelines	More detailed **implementation specific** guidance for how to achieve the requirements defined by the standards
Procedures	Specific step by step documentation of how to perform tasks that achieve the requirements defined by the policy to the level expected by the standards

Policy Components

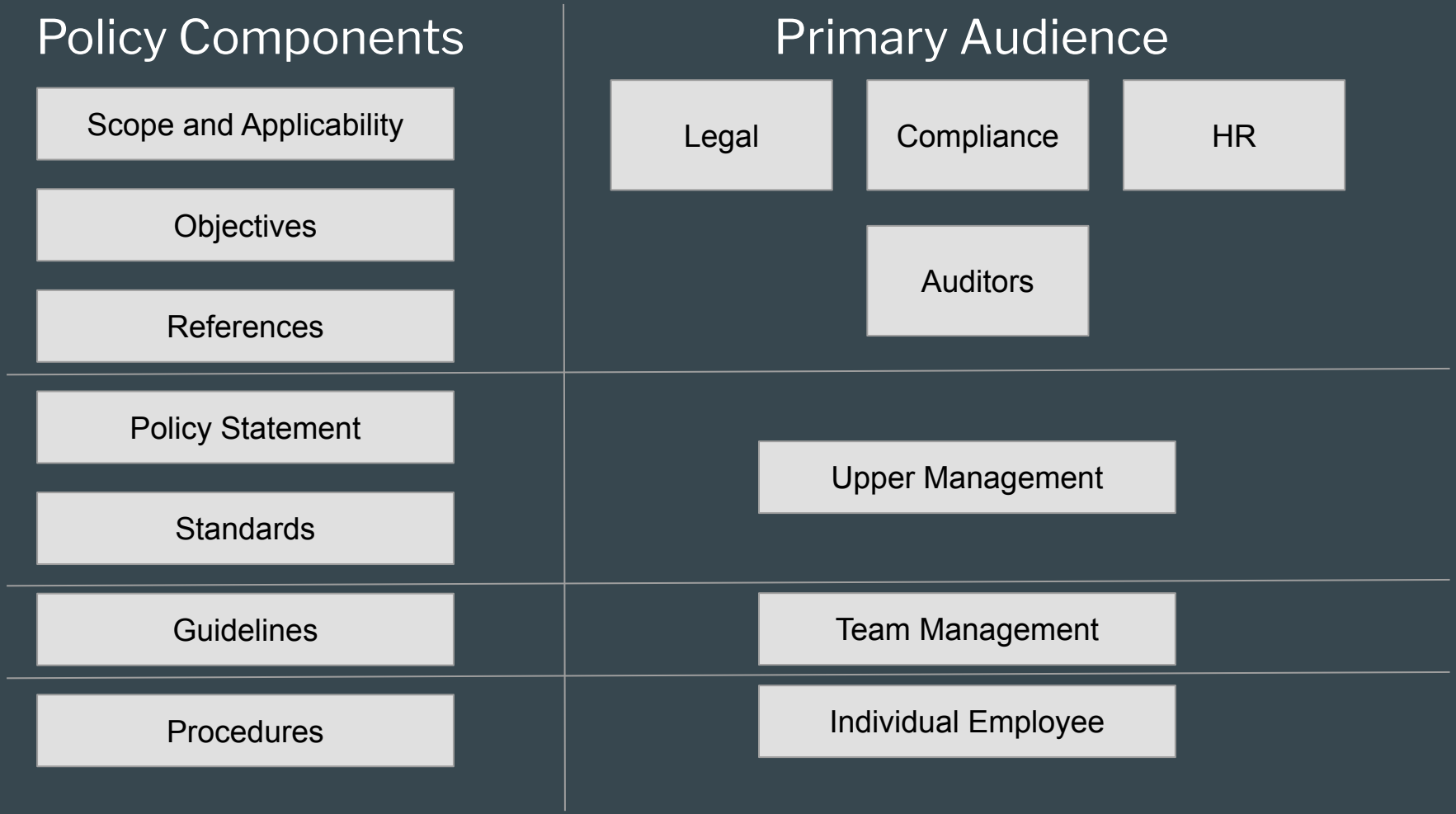
- Scope and Applicability
- Objectives
- References
- Policy Statement
- Standards
- Guidelines
- Procedures

Typical Policy Construction

Lengthy, complex policies that require a legal degree to understand

Disjointed Docs

What If We Decouple These Components By Audience?

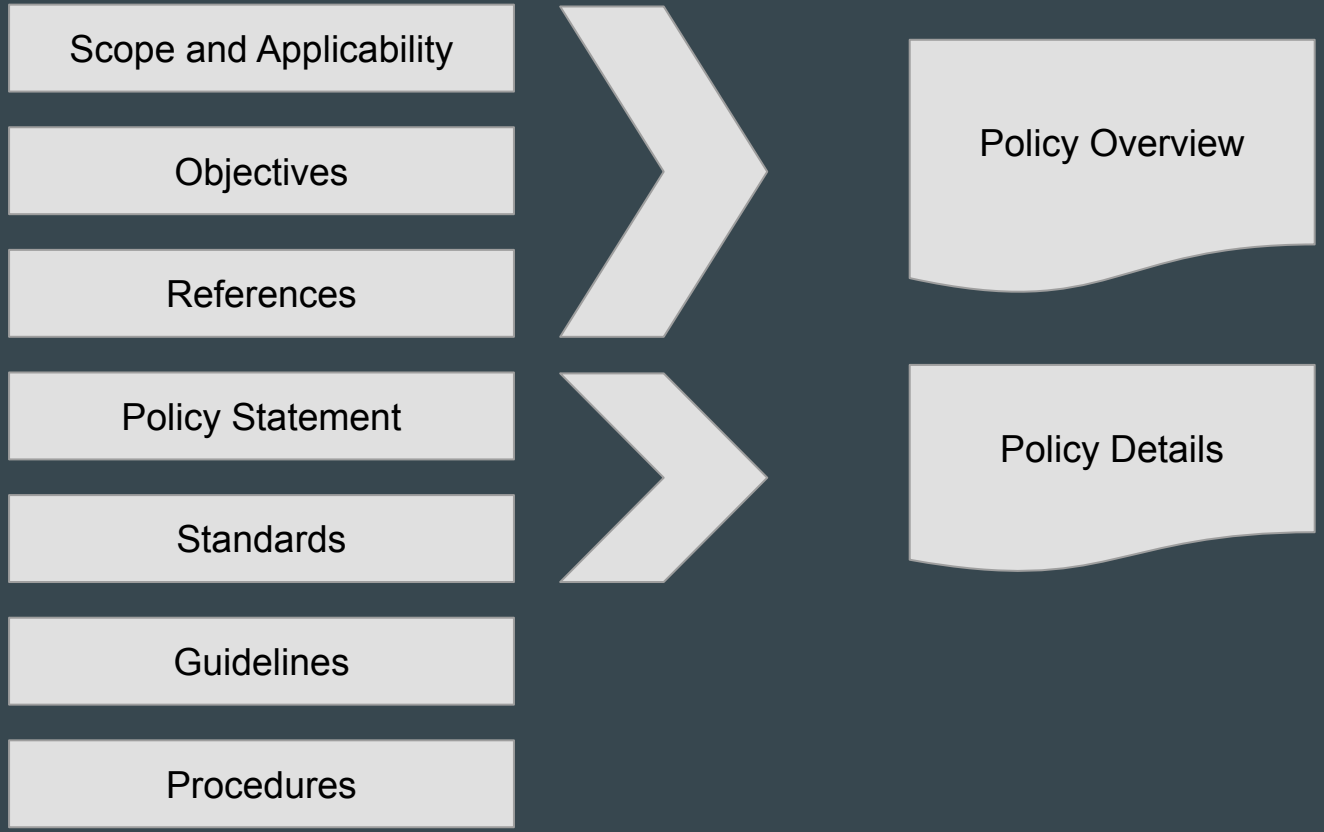

Policy Components
Primary Audience
Scope and Applicability
Objectives
References
Policy Statement
Standards
Guidelines
Procedures
Legal
Compliance
HR
Auditors
Upper Management
Team Management
Individual Employee

Policy Components

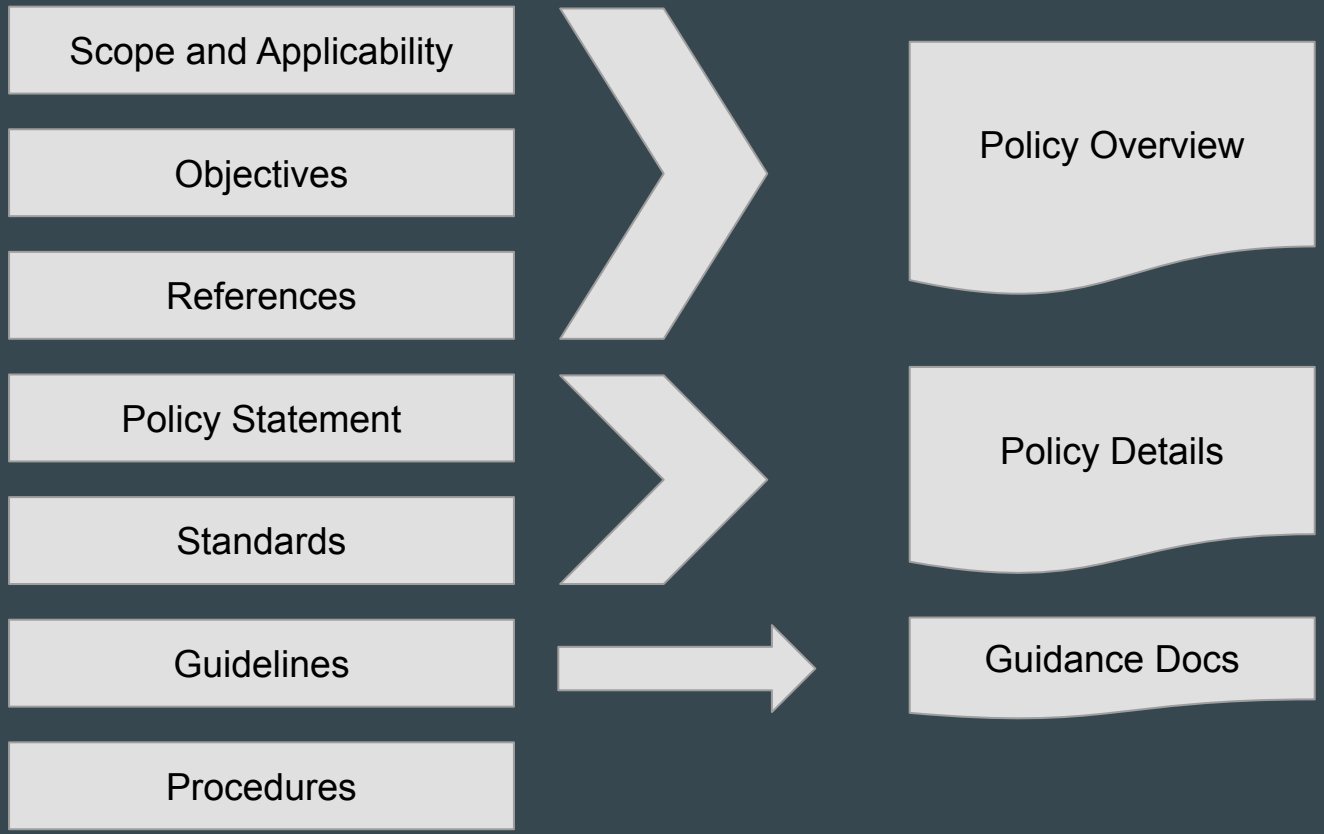
- Scope and Applicability
- Objectives
- References
- Policy Statement
- Standards
- Guidelines
- Procedures

Policy Overview

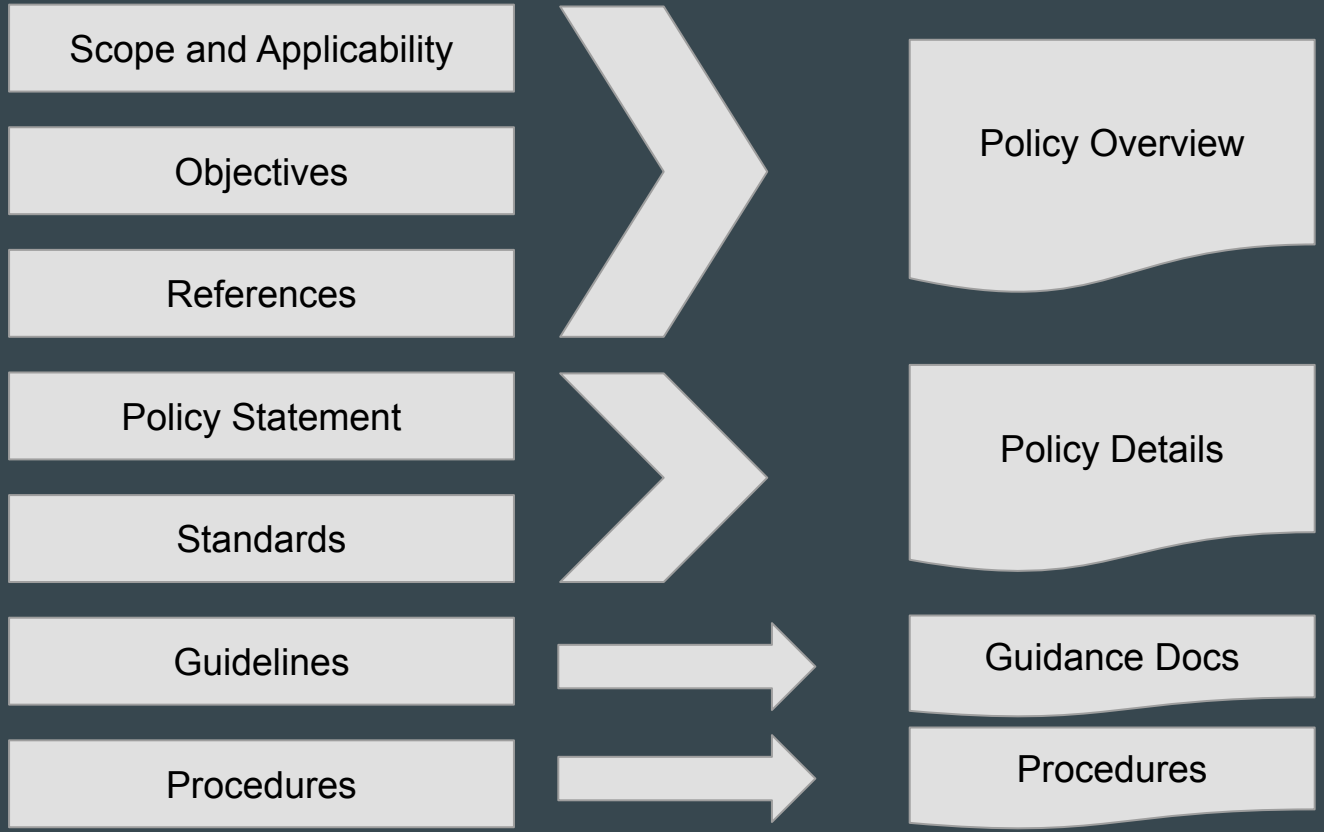
Policy Components



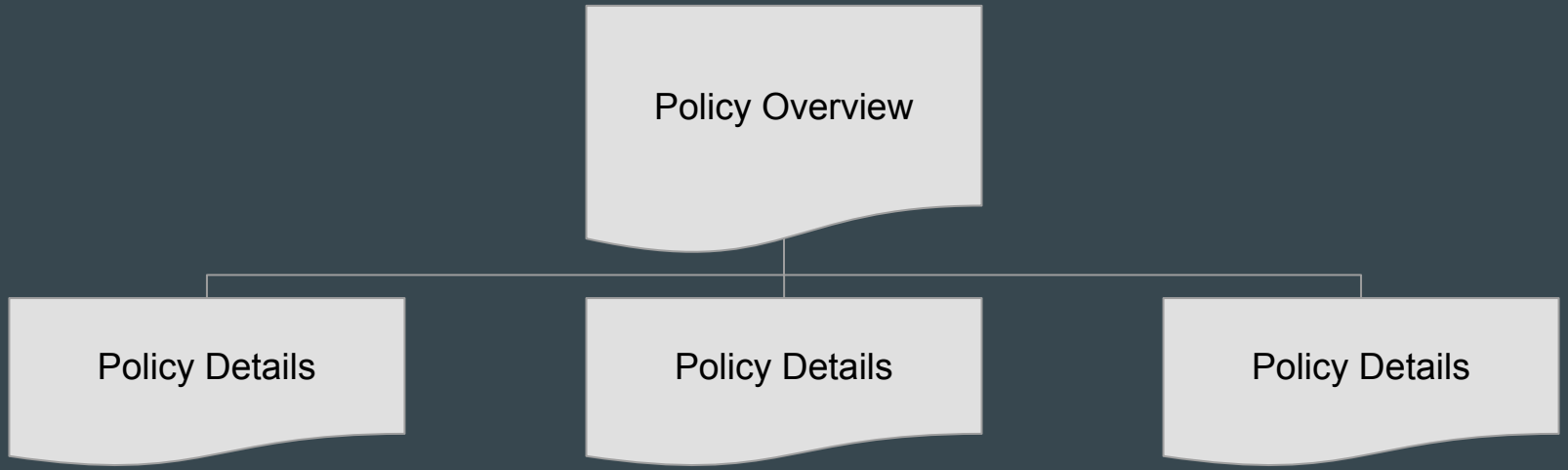
Policy Components

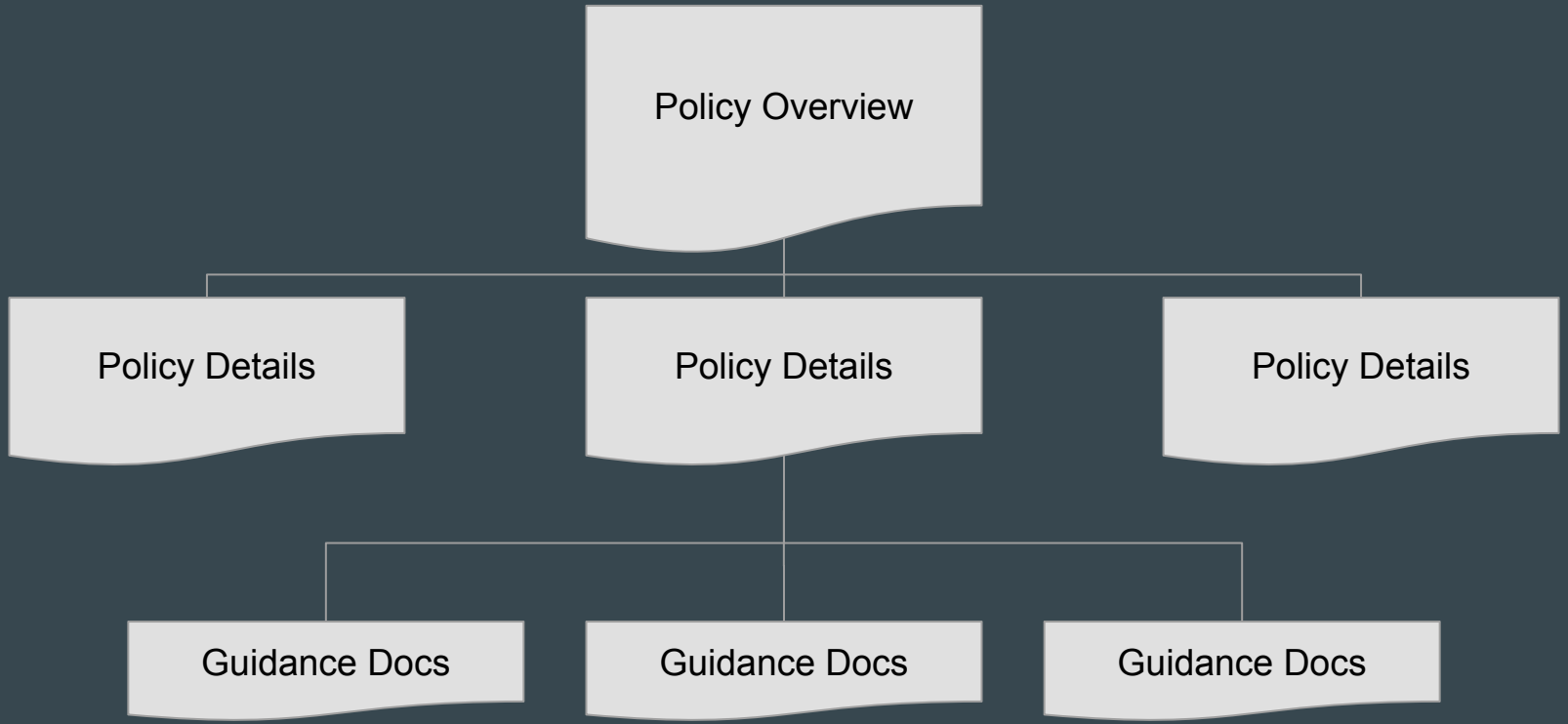


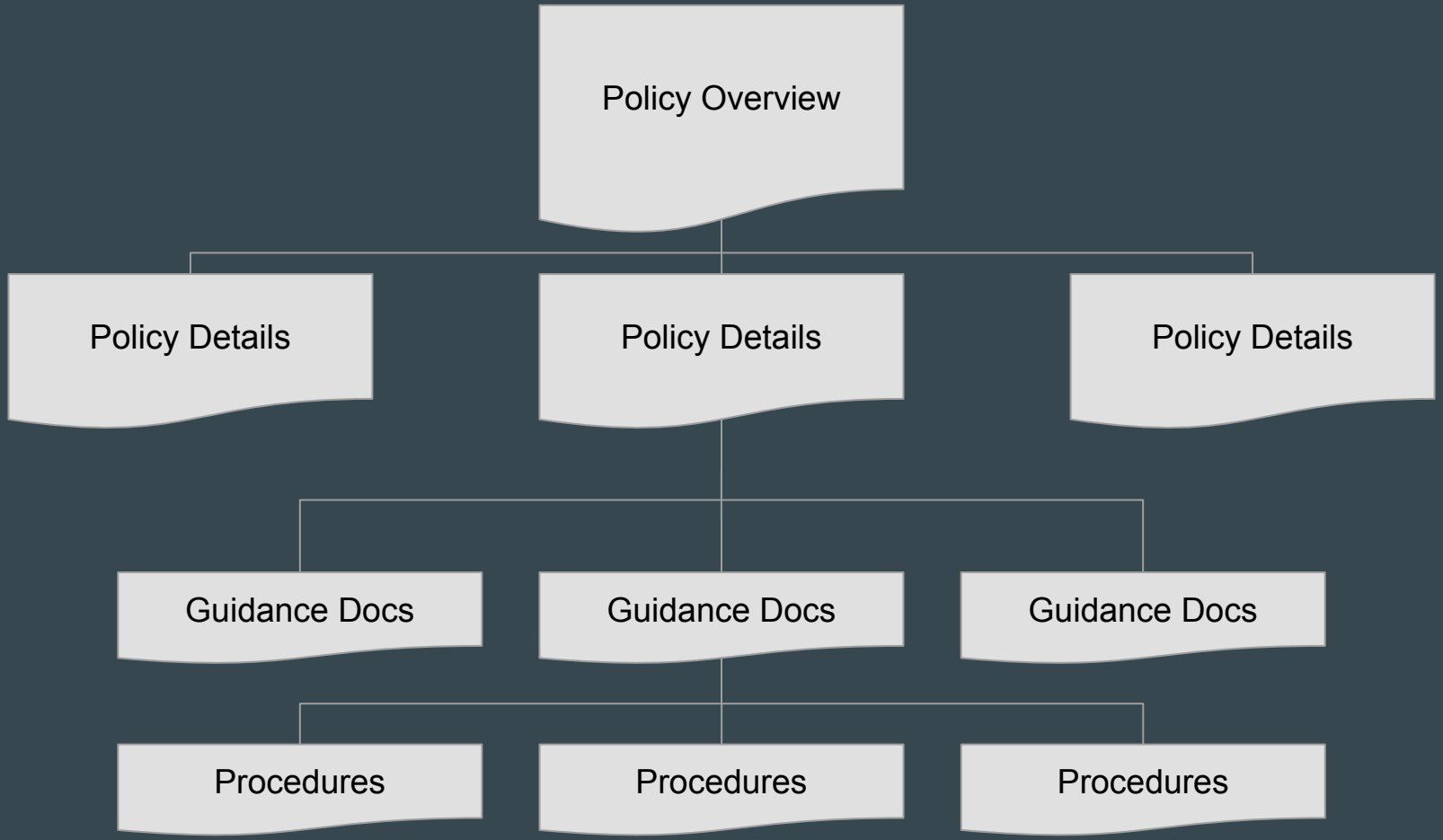
Policy Components



Policy Overview


Policy Overview
Policy Details
Policy Details
Policy Details


Policy Overview
Policy Details
Policy Details
Policy Details
Guidance Docs
Guidance Docs
Guidance Docs


Policy Overview
Policy Details
Policy Details
Policy Details
Guidance Docs
Guidance Docs
Guidance Docs
Procedures
Procedures
Procedures

What Does This Look Like In Practice?

Policy Overview

- Clear and concise single sentences that define the intent for each policy
- Easy to see all available policies and find the one that is applicable
- Useful for:
  - Onboarding
  - Landing page

Information Security Policies

Information Security Policies Overview

Information Security Policy Definitions Glossary

Policy	Policy Statement
Network Security	We shall ensure that all data and systems on our network are appropriately secured.
InfoSec Risk Management	We shall appropriately assess all risks to the business and ensure there is sufficient protection for our company.
Vendor Management Policy	All vendors used by the company must be reviewed for security concerns on a regular basis.
Access Control Policy	Access to company assets must be protected and limited based on the “least privilege” concept.
Data Classification Policy	Data within the company must be tracked, categorized based on sensitivity, and appropriately protected.

Policy Details

- Clear and concise single sentences that define the intent for each policy
- Direct, actionable, implementation agnostic requirements for how things should work
- References to documentation for those who need more information
- Useful for:
  - Providing requirements to teams
  - Quick reference support

Network Security Policy

Information Security Policies Overview

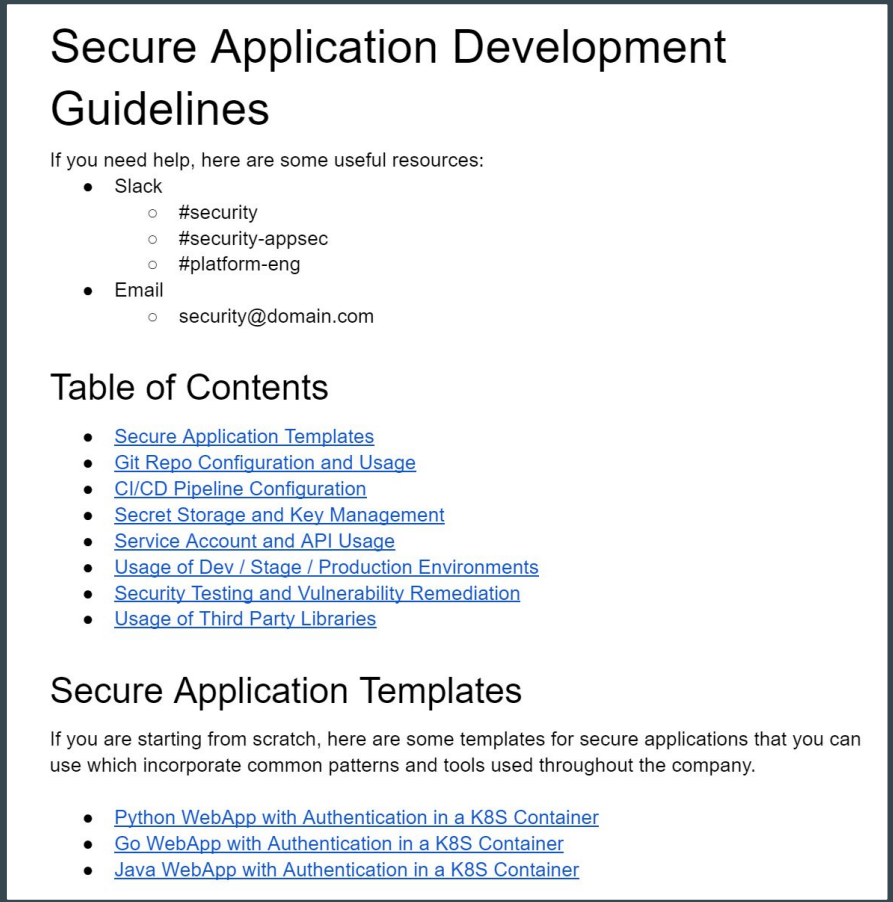
Information Security Policy Definitions Glossary

Policy: We shall ensure that all data and systems on our network are appropriately secured.

- All connections must be encrypted
  - SaaS Configuration Guideline
  - AWS Configuration Guideline
  - GCP Configuration Guideline
- All systems on company owned networks must be appropriately configured and authorized
  - System Configuration Guideline
  - AWS Configuration Guideline
  - GCP Configuration Guideline
- Access to systems and applications must be monitored and secured
  - AWS Configuration Guideline
  - GCP Configuration Guideline
  - WAF Configuration for Networks Guideline

Guidance Docs

- Listing of ways to get help or reach out for more info
- Detailed instructions for how to accomplish specific tasks.
- Links to existing guides and templates
- Setting expectations for things to do, things to avoid, and timelines for remediation
- Useful for:
  - Reference for teams, engineers



Secure Application Development Guidelines

If you need help, here are some useful resources:

- Slack
  - #security
  - #security-appsec
  - #platform-eng
- Email
  - security@domain.com

Table of Contents

- Secure Application Templates
- Git Repo Configuration and Usage
- CI/CD Pipeline Configuration
- Secret Storage and Key Management
- Service Account and API Usage
- Usage of Dev / Stage / Production Environments
- Security Testing and Vulnerability Remediation
- Usage of Third Party Libraries

Secure Application Templates

If you are starting from scratch, here are some templates for secure applications that you can use which incorporate common patterns and tools used throughout the company.

- Python WebApp with Authentication in a K8S Container
- Go WebApp with Authentication in a K8S Container
- Java WebApp with Authentication in a K8S Container

Benefits of This Structure

Document Management

- Documents are decoupled, so they can be individually modified and approved without re-approving the entire set
- Common components (overview, definitions, etc) are referenced on each page and updates are instantly applied to all child documents
- Documents can be compiled for auditors, and are better organized than gigantic single document policies.

Usability and Comprehension

- Only the necessary information, at the appropriate level of resolution, is presented at one time
- Links to further documentation are provided for additional detail where necessary
- Specific requirements can be individually referenced, and documents form a “checklist” for teams to ensure their implementation meets expectations

This Isn’t The End:

Format Doesn’t Matter
if your Content is Terrible

Write Better High Level Policies

- Keep policies and standards **short**, **readable**, and **implementation agnostic**

- Ensure appropriate management buy-in for policies

- Tie your policies to **required controls** and don't go overboard
  - Regulatory control frameworks (HIPAA, GDPR, CCPA, PCI, etc)
  - Industry standards (NIST, CIS, etc)
  - Risk reduction for identified and documented risks

Make Your Guidelines Useful

- Ensure your documentation actually matches your environment
- Provide useful implementation details for devs and engineers
- Work with platform engineering teams to ensure your requirements are supported and integrated -- make it easier to use “paved roads” compared to going it alone
- Always include ways to reach out for questions

Provide the right information

at the right level of detail

to the appropriate audience

Instagram / Twitter

foghorn@NickLeghorn.com

GitHub

Website

Email