



Gemini's Policy Laxative!

The Cure for Policy Constipation
or the care and feeding of a healthy cybersecurity policy

NSF's NOIRLab



It all started with a mouse



If by mouse you mean a Master Information Systems Security Policy and Procedures document (MISPP), which is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk for your Organization. The Cybersecurity Plan, as part of our Cybersecurity Program, incorporates ongoing activities to:

- Develop and maintain relevant policies and procedures
- Assess and review information technology
- Provide cybersecurity training and awareness
- Mitigate prioritized risks generated through periodic audits and assessments



Tip #1



Write policies with a very small group of co-creators! I have found it best to be just me and one other, but should never be larger than 3 total.

The important thing is to keep it light and informal. No such thing as a bad idea. No judging writing while still in flux. Keep it changing and flowing.

You may also want to keep the writing teams consistent when you find a team with good writing rapport.



Collaboration: Co-writing ping pong example

Don't mess with security file stuff. (free flow writing, no judging)

Don't change security file or bypass security measures. (other author revises... back and forth it goes)

Staff shall not change security files or bypass security measures. (who... should or should not... do or don't do something)

Staff shall not alter any security file or setting that would bypass security measures implemented by IT. (getting better)

Staff shall not alter any security file or setting. (make more clear by deleting unnecessary specifications)



Authoring Process

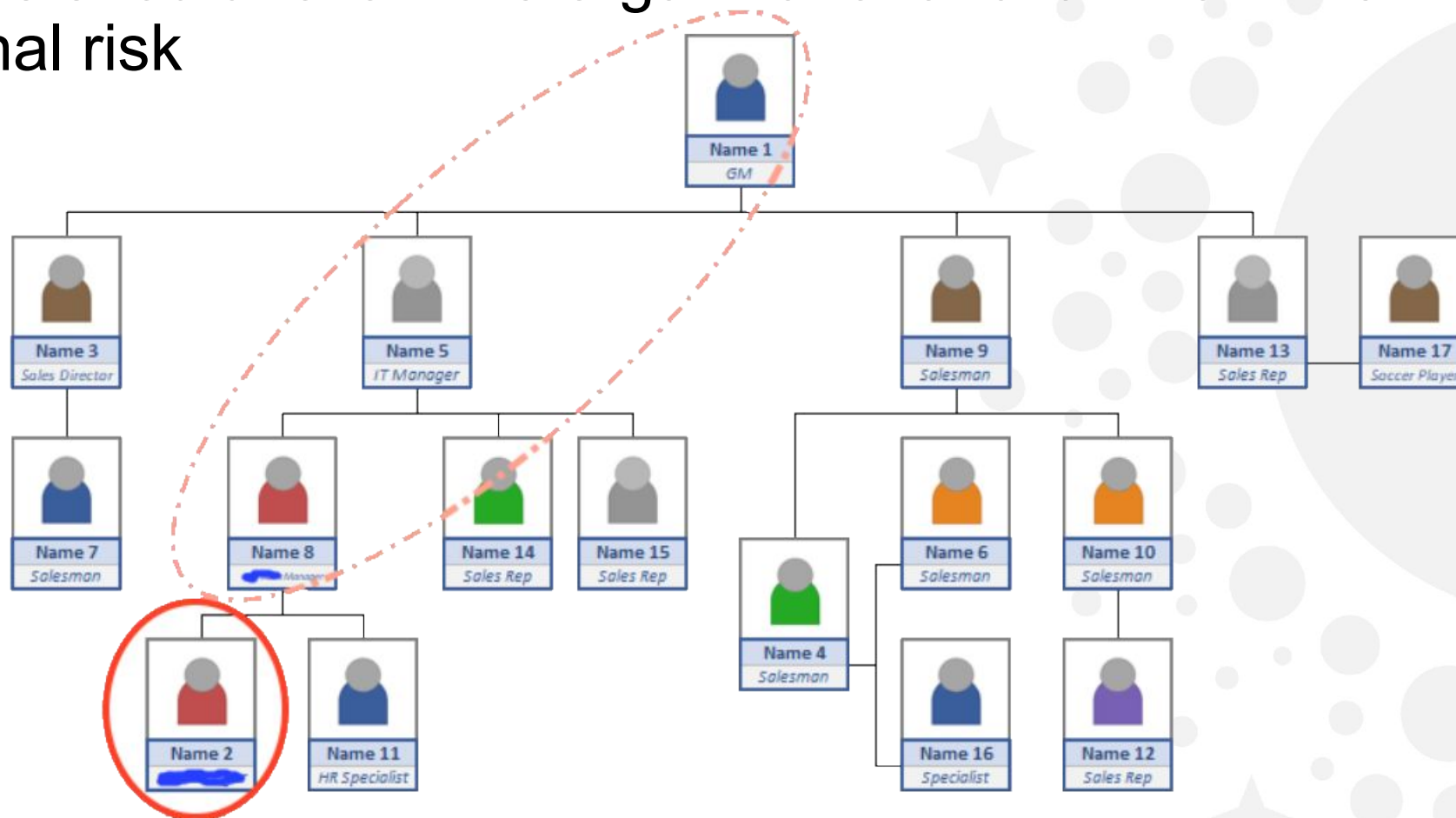
1. Write with limited number of co-creators (2-3 members)
2. Get comments from technical members
3. Clean up version
4. Wait a day or two without looking at the document
5. Have a full read through with co-creator and make last edits
6. Send to document signers for review
7. Once all reviewer comments have been satisfied, create PDF of policy
8. Send to all signers, with Director signing last





TIP #2

Policy approvers should follow the organizational chart from the author to the final risk acceptor, the **Director**.





Final Review Process

- This is not the one novel inside you, don't take change comments personally
- Listen to comments of reviewers
- You don't need to accept every suggestion, but recognize that if they suggested a change that is "not right" that probably means that you need to clarify that part of the policy for better understanding.





Start from where you are



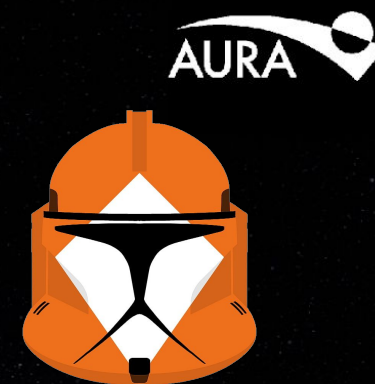
ITIL tells us in the “Seven Guiding Principles” to not start from scratch without considering what is already available to leverage. Avoid re-creating the wheel!

Start your policy by meshing together other sources as a starting doc to start your policy collaboration. Don't start writing policies from scratch.

- Your existing policy, if you have one
- Trusted CI guides and templates: <https://trustedci.org/guide>
- SANS templates: <https://www.sans.org/security-resources/policies>
- Peer or parent organization's policies



Tip #3



Keep wording consistent!

Such as the use of “may”, “must”, or “should”

Just copy, paste, and clone phrases often. This is not creative writing, consistent phrases can actually lead to less confusion, so clone what works.

Either develop a policy template or use your first policy as a template for future policies. Much of the wording and sections of policies are likely to be the same or similar between policies.



Templates



The Green Sheet

The Green Sheet

Name of Policy Here

Status: Version 1 in development

Distribution Restriction: For Distribution to Gemini Personnel Only

Author(s): Chris Morrison, Jerry Brower

Stakeholder(s): Gemini Directorate, HR Liaison


Prepublication Log for Version 1.1:

Date	Description of Changes	Changes Made By
		Jerry

Planned Location for Published Document:
DMT, Gemini Policy Reference Webpage, ITS archive, Gemini's Policy Creation Procedure.

Remove this cover sheet prior to publication. The content for publication begins below.

Policy Template

Name of Policy Here		Element:	Rules of Behavior
	GEMINI OBSERVATORY CYBER SECURITY PLAN	Policy Number:	ITS-POL-00XX
		800-53 Control:	i.e. PL-4
		Revision:	0.1
		Creation Date:	1/29/2018
		Pages:	#

- 1. Purpose**
This document defines ... Describe purpose once Scope and Overview below are complete.
- 2. Scope**
This policy applies to XXX as they pertain to Gemini YYY. Complete after section 5 Policy complete and use headers to help define scope.
- 3. Overview**
Give the executive summary overview of policy here in one paragraph once section 5 Policy is complete.
- 4. Definitions**
 - 4.1. "ITS" or "IT Services" refers to the Information Technology Services Department
- 5. Policy**
 - 5.1. Main sections of policy
 - 5.1.1. Policy topic here
 - 5.1.1.1. Specific policy item.
 - 5.1.1.2. Another item or process.
 - 5.2. Another section
 - 5.2.1. More items.
 - 5.2.2. Here is a URL reference:
<http://dmt.gemini.edu/docushare/dsweb/View/Collection-69742>
- 6. Responsibilities**
 - 6.1. ITS responsibilities
 - 6.1.1. List stuff here



Policy Purpose

“This document defines” stuff...

- i. Describe purpose once Scope and Overview below are complete.
- ii. Use the Scope and Overview to describe why you need this policy and what it does.

By writing this section last, you will have a fully formed picture in your head of the “what it does” of the policy and “why” your org needs it.





Policy Scope

This policy applies to XXX as they pertain to Gemini YYY and ZZZ.

1. Complete after section 5 “Policy” complete and use the policy headers to help define scope of what this policy is defining.

Scope also writes itself by using the policy main headers. Use what you have already done.





Policy Overview

Give the executive summary overview of policy here in one paragraph once section 5 Policy is complete.

- i. If a staff reads nothing else, this should give the gist and main points of policy.
- ii. This is also a good place to provide reference to any master policy or parent policy.

It should also have at the end a reference to your Master Policy. Always keep the big picture in mind. Think and work holistically.



Policy Definitions



“ITS” or “IT Services” refers to the Information Technology Services Department

- i. Start with your standard list
- ii. Go back through your policy and add any acronyms or abbreviations you used with the full name or title.
- iii. Also, remove any standard list items that you ended up not using in you policy text. (doc search is your friend)
 - **“LAN” refers to local area networks**
 - **“NSF” refers to the National Science Foundation**



Policy Main Body

The meat of the policy

- i. Policies in the main body should be in the form of; who must/should do or do not something
- ii. This should be organized by general policy topics
- iii. This is where you copy all the policy stuff from all the sources you are meshing together.
- iv. Then move around the lines to group and sort everything into the topics
- v. Now is when you take all the parts that you like from the various sources, mesh it all together, remove redundancy, copy and paste consistent wordings, etc.



Policy Responsibilities

1. Department responsibilities

- i. The ITS Manager has the management responsibility for all aspects related to IT services, IT policies and any matters related to information security.
- ii. The ISSE acts as the first point of contact for any request for clarification of Gemini Observatory ITS policies and procedures.
- iii. The ISSE coordinates all cybersecurity incident responses, including correspondence with the affected visitor, staff, or user.



Policy Responsibilities (continued)

2. Gemini manager responsibilities

- i. It is the responsibility of every Gemini manager to read, understand, and disseminate information listed in section 5 of this policy to their staff.
- ii. Gemini managers must immediately report any known or suspected cybersecurity incidents or violations of this policy to the ISSE or ITS Manager.



Policy Responsibilities (continued)

3. Gemini staff responsibilities

- i. It is the responsibility of every Gemini staff member to read, understand, and respect the information listed in section 5 of this policy.
- ii. Gemini staff members must immediately report any known or suspected cybersecurity incidents or violations of this policy to their supervisor.

4. Gemini visitor responsibilities

- i. Gemini visitors should report any known or suspected cybersecurity incidents or violations of this policy to their Gemini sponsor.
- ii. Any Gemini visitor that connects their computer equipment to visitor networks that provide only internet access must respect the information listed in section 5 of this policy.
- iii. Any Gemini visitor who has received authorization to connect their computer equipment to internal Gemini Systems must respect this and all other relevant Gemini policies as stated in the Master Information Security Policy



Approvals (Getting it signed)

- Document Owner is author
- Reviewers are for committee chairs or other necessary stakeholders. This is optional and should be used sparingly.
- As mentioned in Tip#2, Policy approvers should follow the organizational chart from the author to the final risk acceptor, the **Director**.

APPROVAL SIGNATURE RECORD		
Reviewer Role	Title	Signature
Document Owner	Author's Title	
Reviewer 1	Other stakeholder?	blank?
Reviewer 2	Try to limit signatures	blank?
Document Administrator	Department Manager	
Approved by:	Associate Director of ???	
Accepted by:	Director	



Technical Suggestions

Here are a few suggestions for handling this process using the tools available.

1. Create a single PDF as final for signature
2. Make folder in cloud storage Drive called “Policies for Signature”
3. Share this with your signature group
4. Send an email with link to the folder share to signature group telling them to please sign

This will ensure that all signatures are on the same PDF file without needing to pass the PDF file one signator to another creating forked versions of the file.



Questions?



Mahalo! (Thanks!)

Now let the policies flow...



Ministerio de Ciencia, Tecnología e Innovación
Argentina