Policy 1.1 : Master Information Security Policy & Procedures

Scalable Cyber Infrastructure for Multi-Messenger Astrophysics

Authors: Warren Anderson, Vladislav Ekimtcov, Margaret Johnson, and Don Petravick

Information Classification: Public

Table of Contents

1 Purpose, Scope, and Applicability

This document represents the core cybersecurity / information security policies for the Scalable Cyberinfrastructure for Multi-Messenger Astrophysics (SCiMMA) Institute, including programmatic commitments, roles and responsibilities; references to other special purpose policies. "Cybersecurity" is defined in Appendix B, and is used interchangeably with "information security" in this policy and for the purposes of the cybersecurity program.

The SCiMMA Institute is currently in a conceptualization phase. As such, the policies and procedures in this document are expected to change frequently. Nonetheless, having clearly delineated information security policies and procedures are key to reaching a level of maturity that will inform opportunities to move beyond conceptualization and become a full-fledged institute.

The SCiMMA Institute is a virtual organization funded by the National Science Foundation (NSF) through a grant to participating institutions. As such, it does not directly employ personnel, but rather recognizes three levels of participation in its activities.

1. SCiMMA Institute Members - NSF funding explicitly identifies one or more individuals at each participating institution, herein designated a SCiMMA Institutional PI. For the purpose of this document and the cybersecurity program, institute members are individuals who are identified by SCiMMA Institutional PI as participating in funded SCiMMA activities. The director of the SCiMMA institute may further designate that organizations who are unfunded are participating institutions and approve the appointment of a SCiMMA Institutional PI from those organizations, who may then designate other individuals as institute members.
2. SCiMMA Collaboration Members - SCiMMA Institute is expected to form close collaborations with other virtual or real organizations via specific memoranda of agreement. Such agreements may entail privileged access to collaboration assets and resources. Each memorandum will identify one or more SCiMMA Collaboration PIs. SCiMMA Collaboration PIs are, in turn, responsible for designating individuals from their organization to be SCiMMA collaboration members.
3. SCiMMA Community Members - SCiMMA's mission is to provide cyberinfrastructure to the astronomy and astrophysics communities. Usage of SCiMMA provided cyberinfrastructure will be dictated by end-user agreements.

The policy applies to all SCiMMA Institute and Collaboration members in relation to their usage and privileged access to SCiMMA Institute assets.

SCiMMA owns no physical hardware assets. SCiMMA services and software assets are hosted via contract (explicit or implicit) with commercial entities such as Amazon, Google, GitHub and CILogon2. Endpoint hardware (laptops) used by institute and collaboration members are the property of participating institutions or individual participants. Therefore, this policy will not cover physical hardware assets, but will apply to virtualized hardware hosted under SCiMMA contracts.

2 Program Elements

This section describes policy and procedures that govern our cybersecurity program. For more information on the cybersecurity program. General information about the program can be found at http://www.scimma.org/.

2.1 Framework

SCiMMA is providing an infrastructure for Multi-Messenger astrophysics with the following external constraints:

- The project builds infrastructure consistent with the EU GDPR regulations., to provide for international participation.
- There are no formal, external compliance requirements originating with funding agencies.
- There are no formal, external compliance requirements induced by astrophysics-related data handled or held by the project.
- The infrastructure must be consistent with astrophysical community expectations for protecting proprietary research data. This includes SCiMMA system meta-data which can be used to infer the activities of researchers.
- Our AWS vendor places information security responsibilities on SCIMMA via the "AWS Shared Security Model"

The framework used is the Trusted CI Framework (trustedci.org/framework).

2.2 Adoption

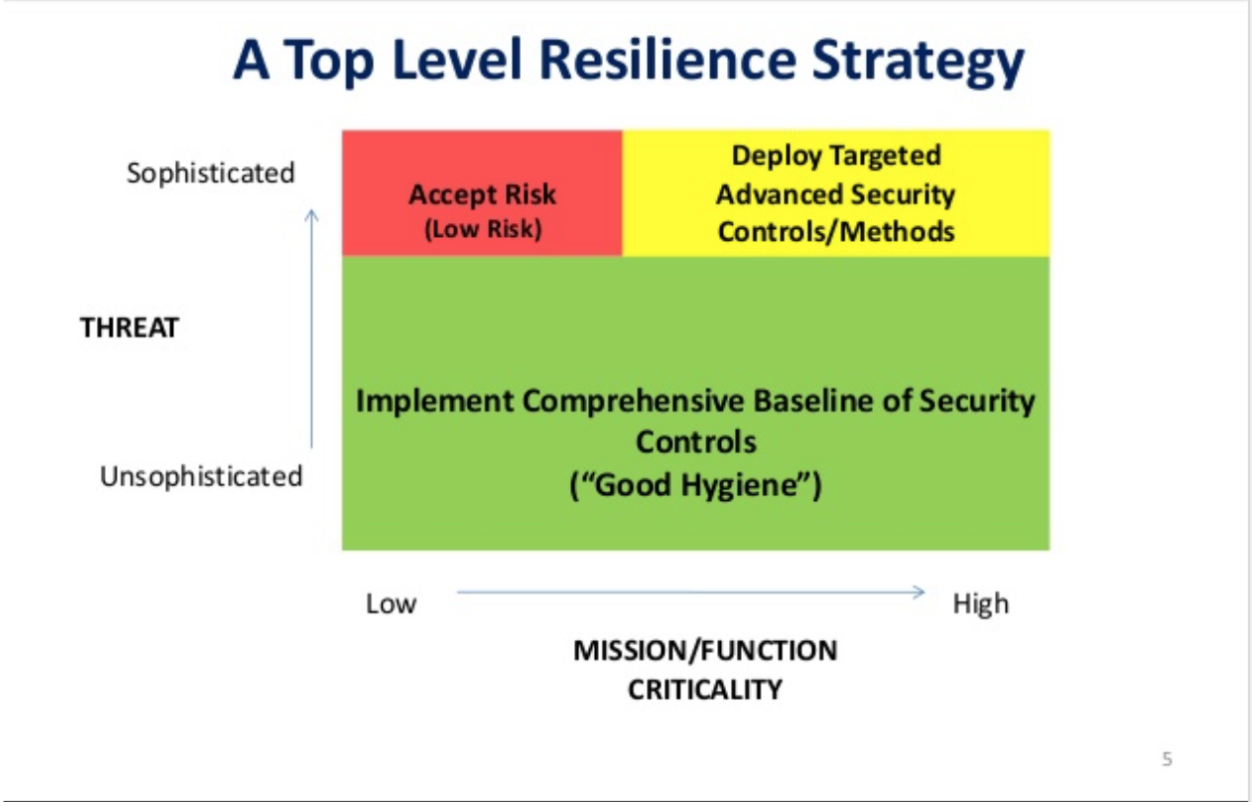
The SCiMMA PI approves the security program laid out in this document.

2.3 Baseline Control Set

SCiMMA has adopted the CIS Controls 6 as our baseline control set. We have also used the crosswalk to version 7 to take advantage of the addition of implementation groups. We will update the version of CIS controls as appropriate.

We supplement the CIS controls with the Open Web Application Security Project (OWASP) Baseline Control set.

CIS v6 baseline controls set the predominant number of assets and focus on the critical assets we have identified. The Gilligan framework (depicted below) is used to identify critical assets which may need additional controls over the baseline..



A Top Level Resilience Strategy

Sophisticated

THREAT

Unsophisticated

Accept Risk
(Low Risk)

Deploy Targeted
Advanced Security
Controls/Methods

Implement Comprehensive Baseline of Security
Controls
("Good Hygiene")

Low

High

MISSION/FUNCTION
CRITICALITY

5

Credit: https://www.slideshare.net/JohnGilligan7/is-cyber-resilience-really-that-difficult

2.4 Policy Development

Conceptualization Phase

For the purposes of this document, the conceptualization phase will be defined to be the duration of the current funding of the SCiMMA project (expected to Q3 of 202?) or until new funding for the project is available.

During the conceptualization phase, SCiMMA Institute security policy has been developed by the security working group. The security working group engaged with Trusted CI to ensure an orderly and complete policy framework, including this document, were identified and prioritized. Engagement with Trusted CI may continue throughout this phase. Members of the security working group work as time allows on policy development and meet on a weekly basis with members of management and dev/ops teams to ensure that security policy and adoption are disseminated and discussed more broadly.

Simultaneously, members of the security working group identify the highest priority cybersecurity need of the SCiMMA Institute guided by considerations of controlling monetary costs, protecting the effort and assets of institute members, and safeguarding the public face of the institute. This includes identifying the highest priority assets of the institute and implementing the highest priority security controls for those assets. Security working group members coordinate with members of the management team and the dev/ops team to ensure that responsibilities of those who are integral to maintaining controls and who are most likely to be impacted by them are understood.

In the final six months of the conceptualization phase, the security working group will:

- Assess the institute's current security posture and identify any unfinished policies or unimplemented controls.
- Estimate the residual security risk for the institute from each of the unavailable policies and/or controls.
- Estimate the monetary and effort cost of finishing the design and implementation of the security program.
- Provide a report summarizing the above to the director of the institute.

Production Phase

For the purposes of this document, the production phase is defined to be the beginning of the next funding cycle for the SCiMMA institute. During this phase, programmatic needs of the institute will require a full cybersecurity program, including the development of policies that were not written during the conceptualization phase and instituting adoption and education efforts, building upon the work done in the conceptualization phase.

2.5 Policy Enforcement

Violations of SCiMMA cybersecurity policies can result in loss of access to resources and services, and/or disciplinary actions though the local PI for Institute Members or responsible party for SCiMMA Collaboration Members, who are accountable to the project for the actions of their staff. Activities in violation of any laws may be reported to the law enforcement authorities for investigation and prosecution.

Suspected incidents must be reported to the Security Working Group by emailing scimma-iam-security-group@uwm.edu. Anyone who believes that there is a violation of a cybersecurity policy or has a related question should contact the Security Working Group. Policy violations investigations are conducted to assure the confidentiality of the reporter when practical.

2.6 Policy Exceptions

While the project expects security policy to be nearly universally applicable, exceptions might have to be made. The existing workflow is to initiate an exception request by bringing it to the attention of the security working group. This request would be discussed at a regular meeting (currently scheduled Monday), appropriate actions would be taken, and the exception would be logged in the project's document management system.

2.7 Programmatic Evaluation

Conceptualization Phase

During the conceptualization phase, programmatic evaluation is largely superseded by programmatic development, but regular opportunities for evaluation will occur. Weekly meetings between members of the security working group, members of the development team and members of the management team dedicated to discussions of security program development and other security concerns will allow members of the security working group to assess impacts of developing security policies and procedures on the mission goals of the institute, and provide an opportunity for management to assess residual risk and direct activities on an ongoing basis.

Concurrently, these meetings will allow the security working group to identify the most pressing gap in the security policy. On an approximately two week cadence, these gaps will be addressed to further develop aspects of the security program, including policies and implementing controls. A primary consideration of this work will be the fit to Dev/Ops activities, preferring policies and controls that can be automated as part of the development work in order to minimize accumulating technical debt in the security program.

One of the gaps that will be under ongoing evaluation is the identification of critical assets and their relationships as they are added to the Dev/Ops activities. The identified risks will be fed into a periodic risk assessments based on the institute's asset inventory.

Production Phase

During the production phase, we expect to hire an Chief Information Security Officer for the Institute. The first duty of the CISO is envisioned to be evaluating the work done during the conceptualization phase by the security working group, including the existing policies and procedures, the asset inventory, and the controls implemented and recommended during conceptualization, as well as the summary of the state of the information security plan developed by the security working group during the final six months of conceptualization. The CISO will then establish priorities for furthering the security program for the institute and communicate these to the director of the institute for comment and approval. One of the priorities is expected to be a periodic review of relevant policies, procedures and implementations assigned to various members and/or working groups within the institute and review and reacceptance of residual risk on an annual basis.

3 Roles & Responsibilities

3.1 Senior Leadership

The SCiMMA PI is also the Director of the SCiMMA Institute. The Director of the institute oversees the entire organization, its progress and the project's relationship to the overall MMA ecosystem. In particular, the PI endorses roles related to information security and notifies the security working group when residual risk is unacceptable. The SCiMMA PI (or delegate) is responsible for collaboration and end-user agreements.

The SCiMMA Institutional Principal Investigators provide staff to the project, and are the people in the project who hold their staff accountable for information security performance. Institutional PIs provide notice for general on-boarding and prompt offboarding of staff to the SCiMMA project and are responsible for identity-proofing members of their institutions during onboarding. Institutional PI's are funded in annual subcontract renewal.

3.2 Activity Leaders

The Chief Architect supplies a series of requirements relating to information security, and works with the Product Owners to schedule stories to assure that information security concerns are adequately resourced and prioritized. The Chief Architect leads the change control function, and tracks the high level services instantiated or relied on by the project.

Each technical Asset has an Asset Owner who is responsible for ensuring that the asset is fit for use and fulfills the needs of the SCiMMA organization, and compatible with the overall architecture articulated by the chief architect. The Asset Owner is responsible for the evolution of the security features within a product, and has a liaison with the security working group.

For software development projects, The Product Owner prioritizes institutional goals and produces “User Stories” which define shippable deliverables for the software development period (“sprint”). The Product Owner serves as an Asset Owner for the Product. Additionally, the individual responsible for marshaling effort towards institutional goals is the Scrum Master. The Scrum Master facilitates the development team’s decision of how to allocate resources within sprints and enables the technical implementation to achieve the User Stories from the Product Owner.

The Activity Leaders described in this section report to the SCiMMA Director.

3.3 Chief Information Security Officer

In the current conceptualization phase of the SCiMMA institute, the Security Working Group works in lieu of a Chief Information Security Officer (CISO) to develop the cybersecurity program. The Security Working Group reports to the Director. We envision a CISO role will be incorporated into the full-fledged institute.

The security working group responsibilities include, but are not limited to:

- Proposes the incremental implementation of security-related policy and procedure documents for the approval by the Director or delegatee.
- Proposes the gradual implementation of security-related policy and procedure documents, guided by the program evaluation discussed in Section 2.6.
- Tracks security requirements flowing from NSF, the cybersecurity community, the MMA community, and ongoing SCiMMA experience.
- Anticipates the needs of a facility offering production services.
- Oversees and staffs security functions drawing internally within the security working group, and also drawing on the project in general.
- Provides an understandable and implementable system.
- Provides core auditing.
- Provides for incident response.
- Acts as a stakeholder in the scrum process - interacts with the product owner to develop stories, participates in sprint planning, participates in sprint retrospective.
- Promotes security-conscious project culture.
- Provides input on permissions needed by user groups in various applications.

- Ensures staff have sufficient resources and knowledge to conduct their business safely.
- Enforces use of technology such as 2FA.
- Maintains the list of Asset-Specific Access and Privilege Specifications and controls, and verifies their implementation.

The members of the Security Working Group are named by the Principal Investigator. As of this writing, the Members of the security working group are:

- Adam Brazier (Ex Officio, as Architect)
- Margaret Johnson
- Don Petravick
- Ron Tapia
- Chris Weaver
- Rich Wolski

The Security Working Group approves security documents on behalf of the Principal Investigator. The Security Working Group attempts unanimous consensus, but may promulgate approval of policies and procedures by ⅘ of its members. The Security Working Group briefs the Principal Investigator of changes in security posture, policy or procedures in a timely manner (at least yearly). The Security Working Group reports out regularly to the all SCiMMA project meeting.

Suspected incidents must be reported to the Security Working Group by emailing scimma-iam-security-group@uwm.edu. Anyone who believes that there is a violation of a cybersecurity policy or has a related question should contact the Security Working Group. Normal business is conducted by liaisons, mentioned above.

3.4 All Organizational Personnel

Each Institute Member or Collaboration Member needs to be familiar with this plan and the detailed policies in Appendix A that are relevant to their work. It is the responsibility of the Institutional PI or Collaboration PI to assure that this plan and the Acceptable Use Policy have been read and understood.

General technical staff require an appropriate understanding of security policy and are responsible for implementing the technical aspects of the security program in the project's technical design process.

Each member is expected immediately to report any known or suspected violations of security policies or procedures, or known or suspected cybersecurity incidents to the Security Working Group or senior leadership.

3.5 Third Parties

A Collaboration Member is a third party who acts according to a collaboration agreement. To the extent the agreement provides for use of SCiMMA resources, Collaboration Members have the same obligations as Organizational personnel, and Collaboration PIs have the same obligations as institutional PI's.

A Community Member is a third party user of SCiMMA cyberinfrastructure. Use of SCiMMA resources will be under terms incorporated into an end-user agreement that will include the Acceptable Use Policy and any other cybersecurity policies relevant to the nature of the Community Members work.

Vendors are third-parties capabilities to SCiMMA, by explicit or implicit contract.

Appendix A: Other Policy and Procedure Documents

In addition to this Master document, SCiMMA has adopted the following additional policies and procedures.

Color key: Has draft, Needed but draft not started, Do not need. The Security Working Group will deliver these documents in the order that is prioritized by the project.

- Acceptable Use Policy - Set of rules that a user must agree to follow in order to be provided with access to a network and/or resources. Used to reduce liability and act as a reference for enforcement of policy.
- Access Control Policy - Defines the resources being protected and the rules that control access to them (ASAPS).
- Adjunct, Subawardee, Subcontractor Policy - An agreement containing a set of rules and expectations to be used between two parties seeking access to the other's network, data or resources.
- Asset Management Policy - Requirements for managing capital equipment including: inventory, licensing information, maintenance, and protection of hardware and software assets (should this include software products like kafka, GitHub, tagging of AWS resources, etc). Consultation with Adam: May not be applicable.
- Information Classification Policy - Used to ensure consistency in classification and protection of data.
- Disaster Recovery Policy - Contains policies and procedures for dealing with various types of disasters that can affect the organization.
- DevSecOps Policy/Software Engineering Policy - see original draft MISPP for software lifecycle phases
- Personnel Onboarding Checklist - Form to be completed at the beginning of employment that addresses authorizing access to resources, physical space and any organizational assets checked out such as laptops.
- Personnel Off-boarding Procedures - Procedure for revoking/reducing privileges
- Personnel Exit Checklist - and form to be completed at the end of employment or change of project status that addresses revoking access to resources, physical space and the return of organizational assets.
- Incident Response Procedures - A pre-defined organized approach to addressing and managing a security incident.

- Mobile Computing Policy - Establish standards for the use of mobile computing and storage devices. (if you have sufficiently critical information on a mobile device, you must inform SCiMMA if the device is lost or stolen).
- Network Security Policy - Outlines the rules for network access, determines how policies are enforced and lays out some of the basic architecture of the company security/ network security environment.
- Password Policy - A set of rules designed to establish security requirements for passwords and password management.
- Physical [and Environmental] Security Policy - Details measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.
- Privacy Policy - A statement that discloses the ways a party gathers, uses, discloses and manages a customer or client's data.
- Remote Access Policy - Outlines and defines acceptable methods of remotely connecting to the internal network.
- Training and Awareness Policy - Outlines an organization's strategy for educating employees and communicating policies and procedures for working with information technology (IT).

Appendix B: Terms and Acronyms

Cybersecurity: "prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation."[1] This definition is scoped to include information assets beyond traditional IT, and includes operational technology.[2]

Appendix -- Revision History

Notify us about issues with this document by filing a ticket here.

Date	Version Number	Status	Description of Change	Initials	Authority
2021-02-09	0.1	Draft	Proposed to Patrick Brady (PI)	WA, VE, MJ, DP	Security Working Group
2021-02-22	0.11	Draft	Removed Reference to "aws provisioning specifics" as salient content is in the incident response procedures as we;	DP	
2022-04-26	0.2	Draft	Revised for presentation to collaboration	DP, MJ	
2022-05-17	0.3	Draft	Responded to comments; revised for presentation to PI	DP, MJ	
2022-05-24	1.0	Approved	Approved by PI and collaboration	PB	PI
2022-05-25	1.1	Approved	Minor editorial changes prior to publishing on SCiMMA website	DP, MJ	Security Working Group

***

This document is based in part on
Trusted CI's Master Information Security Policies & Procedures Template, v3.
For template updates, visit trustedci.org/framework.

[1] https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[2] "Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events." *See* https://www.gartner.com/en/information-technology/glossary/operational-technology-ot