Intersect Security Policy | Security Council

This policy is subject to updates by the Security Council on a regular basis

Roles and bodies

Open Source Committee

The Open Source Committee (OSC) is responsible for setting security policies, but not for administering them. The OSC should not be treated as a trusted body at any point. The responsibilities of the OSC with respect to security are:

- Ensure that there is sufficient security policy in place and that this policy is reflected accurately in the governance structures for Intersect projects.

Technical Steering Committee:

The Technical Steering Committee (TSC) ensures that the governance of Cardano is based upon sound technical awareness and best practices. This body vets, nominates, and appoints all personnel of the Security Council. Ensuring compliance to each specification is met and can serve as an escalation point for the Security Council.

Security Council

The *Security Council* (SC) is a specialized group of key stakeholders and contributors reporting to the Intersect Technical Steering Committee. Members of the Security Council primarily need to be highly trustworthy since they are responsible for overseeing the rest of the security processes. They should be appointed by the TSC on behalf of Intersect, and not elected by Intersect membership.

The Security Council should be trustworthy enough to receive sensitive information, but they should generally only be given it when they need to know it.
The responsibilities of the Security Council are:

- Approve all individuals who are given access to sensitive information around the technical remit of the Intersect's GitHub hosted projects.
    - This may involve background checks and other vetting
    - Know Your Customer (KYC) is needed and provided by Intersect
- Appoint the Security Manager and ensure the role description is updated regularly.
- At least one member of the Security Council should be available and qualified to act as a backup Security Manager
- Appoint Responders and ensure the role description is updated regularly.
- Isolate the rest of Intersect from access to sensitive information
- Ensure that contributors are made aware of security issues where necessary
- Ensure that information on security issues is restricted to those who need to know, and only provided to the extent that is necessary for each role
- Report on responses to security issues to the Intersect Board

Appointments

Appointments are made by Intersect (TSC).
Nomination Criteria:

Technical Expertise

Cardano & Cybersecurity: Deep understanding of Cardano blockchain (architecture, protocols, security features). Knowledge of smart contracts, consensus mechanisms, and transaction validation.

Certifications: CISSP, CISM, CEH, or similar are highly valued, reflecting a solid cybersecurity foundation.

Incident Management: Practical experience in managing and mitigating security incidents in blockchain environments, including use of incident response tools.

Experience

Cybersecurity (3-5 years): Minimum of 3-5 years, specifically in blockchain technologies, focusing on securing networks, applications, and infrastructure.
Incident Response: Proven experience in incident response, root cause analysis, and implementing corrective actions.
Risk Management: Experience in risk assessments, vulnerability identification, and security policy development.

Community Involvement

Cardano Community: Active participation and contributions to open-source projects or security forums within the Cardano ecosystem.

Trustworthiness

Integrity: High level of trustworthiness, essential for sensitive information.
Recommendations: Endorsements from Council members or respected community members.

Commitment

Dedication: Willingness to commit time, attend meetings, and respond promptly to security incidents.
Collaboration: Effective teamwork and communication with Council members.

Communication Skills

Clarity: Strong verbal and written skills for explaining complex concepts.

Documentation: Experience in drafting and reviewing security-related documentation.

Nomination Process

Submission: Nominations by Council members, Intersect board members, or self-nominations.

Review: Council reviews to ensure criteria are met.

Approval: Final vetting by the TSC.

Confidentiality: Nominee identities are kept confidential during the process.

This framework provides a solid foundation for evaluating and selecting candidates with the right mix of technical expertise, experience, and community involvement, while ensuring confidentiality and trustworthiness throughout the process. Certain requirements may be waived for appropriate experience.

Security Manager

The *Security Manager* (SM) is a specific individual reporting to the Security Council. They should be an employee of Intersect, or other highly vetted individual. The Security Manager is responsible for most operational aspects relating to security issues. They are primarily a trustworthy project manager, rather than necessarily being technically qualified.

The responsibilities of the Security Manager are:

- Receive reports of security issues, acknowledge them in a timely manner, triage them if possible, and direct them to the appropriate Responder.
- In collaboration with the Responder, assess and classify the severity of each issue.
- Report on responses to security issues to the Security Council.
    - Sensitive information should be passed up only when and to the extent that is necessary
- Ensure that security issues are followed up on
- Ensure that security-related processes are followed correctly
- Create private channels as needed to discuss or manage security concerns
- Ensure that communication is maintained with the Finder of an issue and that they are aware of the responsible disclosure policy
- Handle administrative tasks, e.g. lifecycle tracking, getting CVEs (Common Vulnerabilities and Exposures), etc.

Appointments

Appointments are made by the Security Council.
Qualifications for the Security Manager:

- Employee of Intersect (or individual under continuity contract)
- Background has been vetted
- Experience of dealing with security incidents desirable
- Relevant technical experience desirable but not required

Finder

The Finder is the person (or persons) who finds and reports a potential security issue. The Finder will usually be a developer, a security researcher, a Cardano user that is external to Intersect, but they could be an employee of Intersect, or even the Security Manager themselves (if e.g. they read a CVE report and realize that it applies to software that is curated by Intersect).

Insider

An *Insider* is an individual who is cleared by the Council to know about sensitive information about a specific project or technical area (security issues, technical reports discussing potential security problems, etc.). The identities of Insiders should not be known except to the Security Manager, the Council, and some number of Insiders as needed (e.g. by the Responder for an issue. Generally, Insiders on the same project should likely know each others' identities).

Insider status should be reviewed regularly and should expire quickly if contributors become inactive or if they show themselves to be insufficiently trustworthy.

Not all Insiders working on an issue need be considered equal; it is up to the Responder to determine which Insiders should be granted which access to information concerning an issue and when.

If a project needs Insiders, then at least one Maintainer should be an Insider.

Insiders should be asked to sign a security-specific NDA, with limited scope relating to security issues.

The responsibilities of an Insider are to:

- Act responsibly with sensitive information
- Follow the instructions of the Responder, which may include additional information discipline
- Follow the Intersect Code of Conduct

Appointments

Insiders will be nominated by the PMC (Project Mgt Committee) for a project, and then vetted by the Security Council.

Qualifications for Insiders:

- Be a Committer on the project

Responder

A *Responder* is an Insider who is the "Directly Responsible Individual" for the resolution (fix or mitigation) of a technical issue. The Responder for an issue need not remain constant; it may make sense to pass it on to someone else at some points.

The Responder is responsible for the complete resolution of the issue. They must ensure that the issue gets all the way to being resolved (including releases, following up to make sure mitigations have been applied etc.).

The position of Responder is a fluid one: if another Insider takes over an issue, then they become the Responder. Some number of default Responders for certain technical areas should be maintained by the SM to ensure that they know who to talk to when there is a problem.

The responsibilities of a Responder are:

- Receive and triage reports of security issues relevant to their area
    - Set the severity level of the issue in discussion with the Security Officer
- Ensure that issues are resolved
    - Formulate a plan to address the issue, bringing in Insiders as needed to help plan or execute
    - Liaise with the SC to bring on additional Insiders if necessary
    - Communicate with the Finder as needed to keep them up to date or seek additional information
- Handle information discipline relating to issues
    - Formulate a communication strategy, if necessary, for referring to an issue in public channels

        - Might be very simple, e.g. “we can acknowledge the issue but no further details”
    - Ascertain and manage which Insiders need what access to the issue, in collaboration with the SM
- Report on their activities to the SM

Policies

Bringing in new Insiders

Insiders should strictly be brought in after vetting by the SC.

In some cases there may be urgency to bring someone in, e.g. if they are doing independent investigation as a community member. In cases such as this we should ask the individual to follow information discipline and promise to move towards making them an Insider on this topic. If they won’t stick to that, they probably aren’t trustworthy enough to bring in anyway.

Issue reporting

The lifecycle of an issue is:

- An issue is reported by the Finder to the Security Manager
- The Security Manager reports this to the Security Council, and then designates a Responder to triage it (this may lead to the Responder changing)
- The Responder collaborates with relevant Insiders to create a plan to address the issue, and to implement it
- The Security Manager monitors the process and ensures that everything is progressing properly and that everyone is kept informed
- The issue is resolved or mitigated
- A confidential report is produced on the issue, explaining its nature, possible impact, defined severity level, and its resolution or mitigation if there is one

- Once the issue is satisfactorily resolved or mitigated so that no threat exists, a public report may be produced in line with the principle of responsible disclosure

Severity

In general, security issues should be treated as maximally severe until triaged by a suitably competent Responder.

Coordinated Vulnerability Disclosure

Following the material in the Cardano Engineering Handbook. Embargo periods may vary depending on the project: for Cardano we will ask people to wait until the fix is in mainnet, which may be a long time. Where an issue reveals other attack vectors, this period may be extended until the threat is deemed to no longer exist.

Example

Here's a longer worked example of what an issue lifecycle might look like.

- Fred (the Finder) reports a serious security issue in Cardano by emailing the security report email address
- Janet (the Security Manager) receives the email, acknowledges receipt to Fred, notifies the SC, and looks for a sensible Responder to start with. Based on a cursory look at the issue, they think it may be related to the consensus layer, so they contact a Responder from that project (Carrie).
- Carrie understands the issue more deeply and instead suggests that Alison take on the Responder role this time.
- Alison triages the issue, tags it as medium severity, and pulls in Xenia and Will (Insiders) to form a plan and fix the issue.
- The team comes up with a fix and also a mitigation.

- Alison and Janet update Fred and the SC on the progress. Fred is informed that while the fix will take until the next HF, once the mitigation is deployed we can responsibly disclose the issue.
- Alison liaises with some SPO Insiders to test the mitigation and later the fix.
- It turns out that there are performance considerations. Alison goes to the SC to ask to bring in one of the performance team as an Insider so they can help.
- Xenia and Will write and test the fix on a private fork, and merge it into the main codebase surreptitiously.
- The full fix goes out in the next HF.
- Once Alison is satisfied that the HF successfully mitigates the issue, and that its disclosure would not create any further security risks, the issue can be disclosed publicly.

Information discipline

Information about security issues should be strictly limited to those individuals that have a need to know about it, and to the extent that is necessary for them to correct verified issues. The Responder is responsible for making sure the policy is clear for any given issue.

Redacting

Project Maintainers are responsible for ensuring that information used throughout issue remediation is kept in confidence and that messages that reveal sensitive information publicly are quickly redacted. In particular:

- Care should be taken when developing code fixes so that the nature of the issue is not revealed prematurely
- Code may need to be obfuscated
- Code comments that reveal the issue should be eliminated
- Github issues should be edited or deleted
- Public Slack messages should be deleted

Users who post such information should be cautioned, and repeated offenses should be considered grounds for a ban from contributing to code repositories. Poor information hygiene with regard to security issues should be a mark against an individual being assigned insider status.

Project development

Security audits

Project Maintainers are responsible for ensuring that any contributions which touch on security are carefully assessed. This may include

- Design review by external experts
- Security audits of the specification, design and/or code

Or other measures as appropriate.

Documentation

All Intersect projects should have a SECURITY.md pointing to this policy.

Disaster recovery for Cardano

Follow and enhance the disaster recovery plan. We may need to fill in some blanks here, e.g. actually how off-chain coordination is done.

Systems

Issue reporting

We will create a durable mailing list for reporting issues, distribution of the list is need to know basis

INTERSECT
UNITING THE CARDANO ECOSYSTEM

Issue tracking

We will use Github Security Advisories; a private issue tracking system with visibility and permissions levels.

Private document store

Some kind of private document store with permission levels so that Insiders can see private docs.

Private communication channels

Private channels for:

- The Security Council
- The Security Manager to talk to
    - Responders (email or other determined platform)
    - Finders (email or other determined platform)
- Responders to talk to Insiders
    - Individually
    - As a team when tackling a problem
- Responders to talk to Finders (email or other determined platform)

We can use private Slack channels or email for most of this. Possibly some of these communications need to be logged for audit purposes? Github Security Advisories also provide a private discussion forum, if that is appropriate?