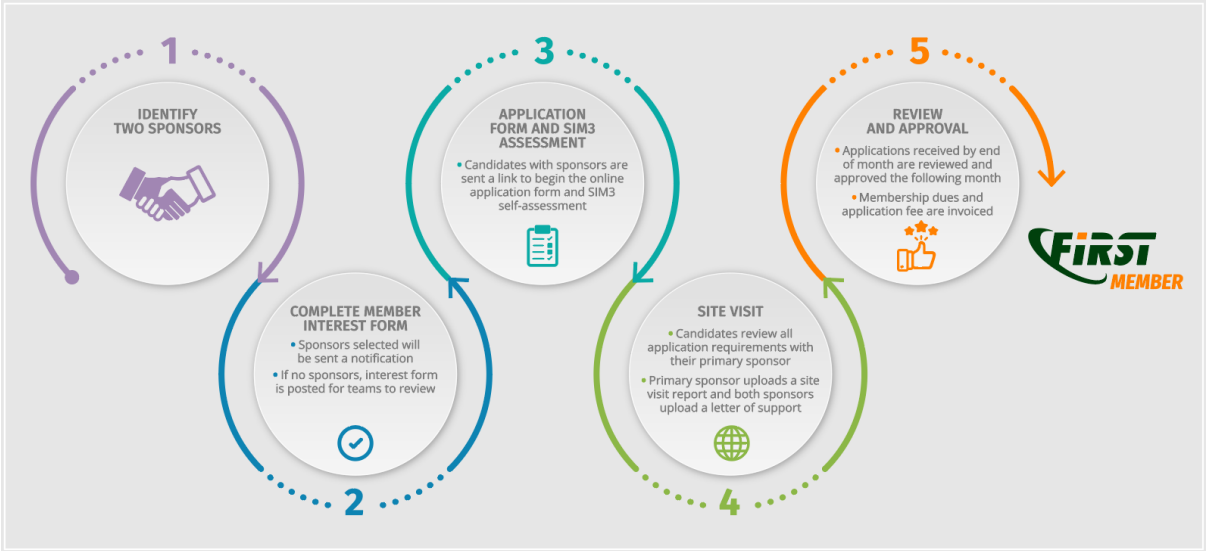
TLP:CLEAR

FIRST Membership Process

Version: 2.1, July 2023



1. Overview

The following is a detailed process of becoming a FIRST Full Member (teams only).

As part of acquiring full membership, two Sponsor teams are needed to support the Candidate team seeking to join FIRST. This document describes the application and sponsoring process, including the Site Visit to the Candidate. The end goal of this process is to become a member and walk the candidate through the process.

As part of acquiring full membership, two Sponsor teams are needed to support the Candidate team seeking to join FIRST. This document describes the Sponsoring Process, including the Site Visit to the Candidate. The end goal of this process is to become a member and walk the candidate through the process.

It is required that the Candidate runs a self-assessment utilizing the Security Incident Management Maturity Model (SIM3). An online tool is available (via the online application form) for this purpose. A subset of the SIM3 parameters must score according to a baseline (see Annex 3), all other parameters are offered for consideration but have no mandatory scores*. The Sponsor should review the self-assessment prior or during the Site Visit or conduct the SIM3 assessment with the team they are sponsoring.

The Candidate must support and host the Site Visit, which is performed by the Primary Sponsor. The Site Visit results need to provide FIRST with enough assurance that the Candidate **meets all requirements** to become an active and beneficial member of FIRST. A site visit report must be provided for all applications starting in August 2023. A site visit report template (Annex 7) is provided for reference and can be modified by the sponsors as needed.

In the next section, the Sponsoring Process is described in detail, whereas the Site Visit is detailed in Annex 2.

** Note that SIM3 is primarily geared for cybersecurity incident management teams of all kinds. However, the focus is only on a subset of the SIM3 parameters, and that subset also applies to e.g. PSIRTs. See Annex 3.*

A high-level view on the process with the steps, stakeholders, and estimated duration is presented on Annex 8.

2. Application and Sponsoring Process

The process is composed of 15 steps with a global estimated duration of 7 months. Depending on the experience of the applying Team, and the Sponsors, this can take shorter. There is no formal minimum duration for the application process.

Please note that:

- Throughout the process, Sponsors are strongly advised to interact with the Candidate as needed and provide support.
- Whenever needed, the Primary Sponsor can get in touch with the Secondary Sponsor for joint consultation.
- If additional guidance or technical support with the FIRST portal is needed, the Sponsors can contact the FIRST Secretariat, for further advice.
- A Candidate can change Sponsors at any time.

Step 1: A team wishes to become a FIRST Full Member and completes the *Membership Interest Form*

This is the starting point. We refer to this team as “the Candidate”. The Candidate will create a profile for the FIRST Portal and then complete the Membership Interest Form which will be submitted to the FIRST Secretariat.

Step 2: Candidate must find two FIRST full members who agree to act as Sponsors. The application process cannot proceed without sponsors.
The Candidate may review the list of current teams to find sponsors. It is recommended that Candidates reach out to teams they have worked with or who are in their industry/region. The Primary sponsor should be from outside the Candidates host/parent organization. The FIRST Secretariat and Membership Committee (MC) may be contacted to assist with introductions if needed but the team should provide suggested teams in their region or with whom they have worked/collaborated.
Estimated duration – 1 month

Step 3: Candidate prepares and schedules the site visit with their primary sponsor
Prior to the site visit the candidate may review the Site Visit template report to prepare the requested materials/documents for review and ensure enough time is reserved to cover all topics.
Estimated duration – 1 week

Step 4: Candidate performs a SIM3 self-assessment
Prior to or during the Site Visit, the Candidate runs a self-assessment utilizing the Security Incident Management Maturity Model (SIM3). This is supported by an online tool within the online application form. Results of the SIM3 self-assessment MUST be reviewed by the primary sponsor.

A subset of the SIM3 parameters needs to score according to a baseline (see **Annex 3**), all other parameters are offered for consideration but have no mandatory scores. After conducting the self-assessment, the Candidate shares the result with both Sponsors to identify potential areas that they should clarify or work on before the Site Visit. Prior to submitting the application, the Open Actions tab in the SIM3 tool should read 0 indicating completion.
Estimated duration – 1 week

Step 5: Primary Sponsor conducts Site Visit
How to perform the Site Visit is described in more detail in **Annex 2**. A base template of the report is available at **Annex 7**. This report is required for all applying teams as of January 2023.

From 1st November 2021, the SIM3 approach is used to validate whether the required subset of parameters scores sufficiently.
Estimated duration – 1 day

Step 6: Candidate completes the Full Member Application Form
The Candidate ***must*** gain access to the FIRST Membership Application Form on FIRST Portal.

Next, the Candidate must fill out the *Full Member Application Form*: an overview of all mandatory and optional fields to fill out is given in **Annex 1**. The Sponsors (and the Mentor, if applicable) will help fill this out, if needed. The application statement in the form replaces the need for a separate application letter from the candidate. The statement should include the reasons they want to join FIRST and the benefits they intend to bring to the FIRST community. They share this with both Sponsors.
Estimated duration – 1 month.

Information provided in the application form will be used to update the teams profile in the FIRST Portal. By applying to FIRST, the candidate agrees to review this information annually for accuracy and provide regular updates to team details and confirm team members.

Step 7: Sponsors review candidacy
The Primary Sponsor informs the Secondary Sponsor on the Site Visit results. Both validate these, as well as the application letter, the Full Member Application Form as filled out in full by Candidate (see the overview in **Annex 1**), and the PGP/GPG keys. At this stage Candidate needs to have assigned both Team Reps (Primary and Secondary), and both may have PGP/GPG-keys (optional), along with the Team's key.
Estimated duration – 1 week

Step 8: Sponsors write supporting letters and Site Visit report
The Primary Sponsor also finalizes the Site Visit report, **including** the assessment of the required subset of SIM3 parameters. Both Sponsors must validate the application package which includes:

- the outcome of the Site Visit
- the validation of the SIM3 parameters
- all accompanying materials

Once both Sponsors are confident with the eligibility of the Candidate as future member of FIRST, they write and upload their letters of support recommending the Candidate for full membership. Sponsors can use Annex 4 as a starting point for their letters. Sponsors have the option to highlight any potentially questionable issues.
Estimated duration – 1 week.

Step 9: All materials are submitted for review.
Sponsors or Candidate upload on the FIRST portal and then submit the Full Member Application Form. This is the final step from the Candidate and the Sponsors.
Estimated duration – 1 day

Step 10: Candidacy compliance check by the FIRST Secretariat
The Secretariat checks the submitted Full Member Application Form monthly on completeness and validity of the Application package. If necessary, interaction with Candidate and Sponsors is activated.

Once all is in order, the application is passed on to the Membership Committee for review.
Estimated duration – 1 month, maximum of 2 months in case of issues

Step 11: Membership Committee review
The MC reviews the application. Once the MC is confident to move forward, it recommends the FIRST Secretariat to accept the application. In case of issues with any component of the Application Package, the MC provides detailed feedback. In case of issue, go to step 13.
Estimated duration – 2 weeks

Step 12: Review by Membership and Board
The FIRST Secretariat submits the application (including the MC recommendation) to the FIRST teams mailing list. If no issue is raised FIRST Secretariat submits the application to the Board. In case of an issue, go to step 13.
Estimated duration – 2 weeks

Step 13: Application feedback and reapplication (if needed)
If any issues or objections are identified during the application process, the FIRST Secretariat takes this back to the Candidate and the Sponsors for resolution – involving the Mentor if one was appointed.

If needed, the process loops back to step 7. In case Candidate and Sponsors fail to solve issues/objections, the application gets rejected, and Candidate and Sponsors are formally informed thereof.

Rejected teams have the right to re-apply, after they can convincingly explain to the FIRST Secretariat, together with their Sponsors (and the previous Mentor, if one was appointed), that the situation has changed enough to warrant a new application. If needed, the Secretariat will consult with the FIRST Membership Committee.
Estimated duration – 2 months

Step 14: FIRST Board votes on application
Once everything has been successfully validated, the Board votes on approval of the Candidate's application, and this is duly noted in the minutes. If approved, proceed to step 15. If not approved, go back to step 13.
Estimated duration – 1 to 2 months

Step 15: Notification
FIRST Secretariat notifies the Candidate and the Sponsors of the approval and sends the "Welcome Package" to the new Full Team member. All members are notified of the success of the Application.
Estimated duration – 1 week

3. Further reading/resources

The following documents are recommended as they provide useful information to Candidates, or even to Teams once members of the FIRST community.

- FIRST: Membership fees www.first.org/membership/#Fees
- FIRST: Teams List www.first.org/members/teams
- FIRST: Current applications for review (members only) portal.first.org/application
- FIRST: CSIRT Services Framework www.first.org/standards/frameworks/csirts
- FIRST: PSIRT Services Framework www.first.org/standards/frameworks/psirts
- FIRST: TLP www.first.org/tlp
- FIRST: Code of Ethics ethicsfirst.org
- OpenCSIRT Foundation: SIM3 portal opencsirt.org/csirt-maturity/sim3-and-references
- RFC 2350: Expectations for Computer Security Incident Response datatracker.ietf.org/doc/html/rfc2350

Annex 1 – Application Checklist

The checklist below corresponds with the Full Member Application Form on the FIRST website.

Item	Mandatory/Optional
A brief statement of why the Team would like to join FIRST and how it plans to participate – application letter	Mandatory
Primary Sponsor – FIRST full member – uploaded on the portal	Mandatory
Primary Sponsor Sponsoring Letter – uploaded on the portal	Mandatory
Secondary Sponsor – FIRST full member – uploaded on the portal	Mandatory
Secondary Sponsor Sponsoring Letter – uploaded on the portal	Mandatory
Site Visit Report and SIM3 Assessment – uploaded on the portal	Mandatory
Team Information ▪ Team Name – this is usually an acronym like CERT-XXX ▪ Official Team Name – the full name ▪ CSIRT Type – Academic, Government, Industry, National, PSIRT ▪ Host Organization – where the team is residing in ▪ Country of Team – main country where the team is based in ▪ Date of Establishment ▪ *Optional: Other Countries of Team* ▪ *Optional: Website*	Mandatory (*optional* where indicated)
Team Members ▪ Fill this out completely for the Primary Representative, Public PGP Key is optional ▪ Fill this out completely for the Secondary Representative, Public PGP Key is optional ▪ *Optional to fill this out for other Team Members (Public PGP Key recommended then, not mandatory)*	Mandatory (*optional* where indicated)
Contact Information • Regular telephone number • Emergency telephone number • E-mail address • Postal address • *Optional: Facsimile number, Other communication facilities, Max response time, Escalation path*	Mandatory (*optional* where indicated)
Constituency ▪ Type of Constituency ▪ Source of Constituency ▪ Description of Constituency	Mandatory (*optional* where indicated)

Item	Mandatory/Optional
▪ Countries of Constituency ▪ *Optional: Internet domain and/or IP address range describing the constituency, Constituency AS numbers,* *IP addresses ranges within constituency, DNS within constituency,* *Additional constituency links (URLs)*	
Services based on FIRST Services Framework ▪ **CSIRT Framework** **Service Area: Information Security Event Management** • Service: Monitoring and Detection • Service: Event Analysis **Service Area: Information Security Incident Management** • Service: Information Security Incident Report Acceptance • Service: Information Security Incident Analysis • Service: Artifact and Forensic Evidence Analysis • Service: Mitigation and Recovery • Service: Information Security Incident Coordination • Service: Crisis Management Support **Service Area: Vulnerability Management** • Service: Vulnerability Discovery/Research • Service: Vulnerability Report Intake • Service: Vulnerability Analysis • Service: Vulnerability Coordination • Service: Vulnerability Disclosure • Service: Vulnerability Response **Service Area: Situational Awareness** • Service: Data Acquisition • Service: Analysis and Synthesis • Service: Communication **Service Area: Knowledge Transfer** • Service: Awareness Building • Service: Training and Education • Service: Exercises • Service: Technical and Policy Advisory ▪ **PSIRT Framework** **Service Area: Stakeholder Ecosystem Management** • Service: Internal Stakeholder Management • Service: Finder Community Engagement • Service: Community and Organizational Engagement • Service: Downstream Stakeholder Management • Service: Incident Communications Coordination within the Organization • Service: Reward Finders with Recognition & Acknowledgement • Service: Stakeholder Metrics **Service Area: Vulnerability Discovery** • Service: Intake of Vulnerability Reporting • Service: Identify Unreported Vulnerabilities • Service: Monitoring for Product Component Vulnerabilities • Service: Identifying New Vulnerabilities	Mandatory to acknowledge what applies

Item	Mandatory/Optional
• Service: Vulnerability Discovery Metrics **Service Area: Vulnerability Triage and Analysis** • Service: Vulnerability Qualification • Service: Established Finders • Service: Vulnerability Reproduction **Service Area: Remediation** • Service: Remedy Release Management Plan • Service: Remediation • Service: Incident Handling • Service: Vulnerability Release Metrics **Service Area: Vulnerability Disclosure** • Service: Notification • Service: Coordination • Service: Disclosure • Service: Vulnerability Metrics **Service Area: Training and Education** • Service: Training the PSIRT • Service: Training the Development Team • Service: Training the Validation Team • Service: Continuing Education for all Stakeholders • Service: Provide Feedback Mechanisms	
Information Handling Policies ■ How is information handled, especially with regards to exclusivity? – needed as any CSIRT/PSIRT team must be able to handle information confidentially ■ What considerations are adopted for the disclosure of information, especially incident related information passed on to other teams or to sites? – the reply here should include the team's support and usage of TLP. ■ *Optional: How is incoming information classified? Are there any legal considerations to take into account with regards to the information handling? Policy on use of cryptography to shield exclusivity & integrity in archives and in communications, especially email, Disclosure policy URL, Product support policy URL*	Mandatory (*optional* where indicated)
Cryptography ■ *Optional: PGP public key – here the team-key is asked for: the keys for the Team Reps have been specified under their contact information*	*Optional*
FIRST Mailing Lists ■ FIRST Teams list – the email address to subscribe to the email distribution list that holds all FIRST members ■ *Optional: FIRST Representatives email – the email address to subscribe to the email distribution list that holds all FIRST representatives (and FIRST staff).* **Note:** *by default, the two Team Reps are added to this list, hence this entry is optional and can be used in case the team wishes to specify a*	Mandatory (*optional* where indicated)

Item	Mandatory/Optional
functional address here ■ *Optional: Allowed posters* **Note:** *by default the FIRST mail servers will accept all mails sent to FIRST lists that come from the teams' main domain name (e.g. csirt-fantasy.org), hence this entry is optional and can be used when the team needs to allow other "posters" as well who are not covered by the default*	
Invoice Information ■ *Optional: PO or Ref. – Specify a Purchase Order number or a reference that needs to be included in the invoices for your team* ■ *Optional: VAT – specify the Team's organization VAT number if it is relevant to have it appear on the invoices for the Team* ■ *Optional: Bill to a different address? – "no" by default, meaning the team address will be specified on the invoice; choose "yes" if you need a different address on the invoice, and then specify that address in the next 3 fields* ■ *Optional: Billing Contact, Billing E-mail, Bill To*	*Optional*

Annex 2 – Site Visit Procedure

The Primary Sponsor visits the Candidate's premises, with the goal of verifying if the Candidate meets the FIRST membership requirements. The Site Visit can be performed virtually instead of in-person, using videoconferencing tools (audio only is not permitted). The Secondary Sponsor is welcome to participate in the Site Visit, either in person or online.

During the Site Visit the Sponsor(s) review the Candidate's organization, processes, tools, systems, premises, etcetera, to gain a thorough understanding on the Candidate's readiness to become a full member of FIRST. This understanding is necessary to enable the Sponsors to support the Candidate's application.

The organization of the Site Visit is up to the Primary Sponsor. The following 6 items are the ingredients:

- 3 of them mandatory: items 1, 3, and 5
- 3 of them are optional, but strongly encouraged: items 2, 4, and 6

1 – Mandatory – The Candidate is evaluated against a subset of SIM3 parameters
The **11** mandatory parameters to review are O-1, O-2, O-3, O-4, O-5, O-10, H-1, H-2, H-7, P-1, P-11. The baseline is set to minimum levels that must be met by Candidate are shown in Annex 3. The online tool is tailored to facilitate this process and a link is accessible in your online application form.

2 – Optional – Discussion of the remaining SIM3 parameters Optional, but strongly encouraged
Such a discussion (the same tool can be used as basis) will be beneficial both for the Candidate and their understanding on how to further advance their team maturity, but also for the Sponsor(s) to gain deeper understanding of the Candidate. (See Annex 3 for all SIM3 parameters) Note: the current version of SIM3 still focuses on CSIRTs of all kinds. Some potential members, like PSIRTs, will fall more or less outside that categorization – in that case, still most SIM3 parameters will apply, and the discussion will still be beneficial, but enough flexibility needs to be exercised by the Sponsor(s).

3 – Mandatory – Candidate and Sponsors to assess the Full Member Application Form
This is to see if Candidate has supplied or can supply all the necessary information and discuss where needed. PGP/GPG keys and the usage of PGP/GPG inside the FIRST community are part of the discussion.

4 – Optional – Sponsor(s) to discuss TLP and the FIRST Code of Ethics with Candidate Optional, but strongly encouraged.
Neither are mandatory, however FIRST strongly recommends to all their members to respect and support both.

5 – Mandatory – Sponsor(s) to assess whether Candidate is in the position to become a full member of FIRST and be an asset to the FIRST community
Sponsors, to their best professional judgment, must assess whether Candidate has the values to become a full member of FIRST and will be able to bring value to the FIRST community. The matter of "trust", basics to how the FIRST community functions, must be thoroughly discussed with the Candidate.

6 – Optional – Sponsor(s) to assess with Candidate its security and confidentiality situation Optional, but strongly encouraged
Sponsor(s) are strongly encouraged to assess together with Candidate the security/confidentiality situation that Candidate is in – regarding premises, access control, separate room(s), network, and system security, etcetera – both physical security and cybersecurity wise.

There are no absolute rules to give here, as much also depends on the kind of environment that Candidate is in. For a university CSIRT the reasonable demands will differ from those for a bank or government team. The end goal is to ensure that the Candidate has a reasonable ability to keep FIRST information confidential. Sponsor(s) can help Candidate in this regard, also to increase the awareness of Candidate (and their governance) for these issues. In the case that Sponsor(s) have grave concerns about such issues, that Candidate cannot take away, these must be highlighted in the Site Report.

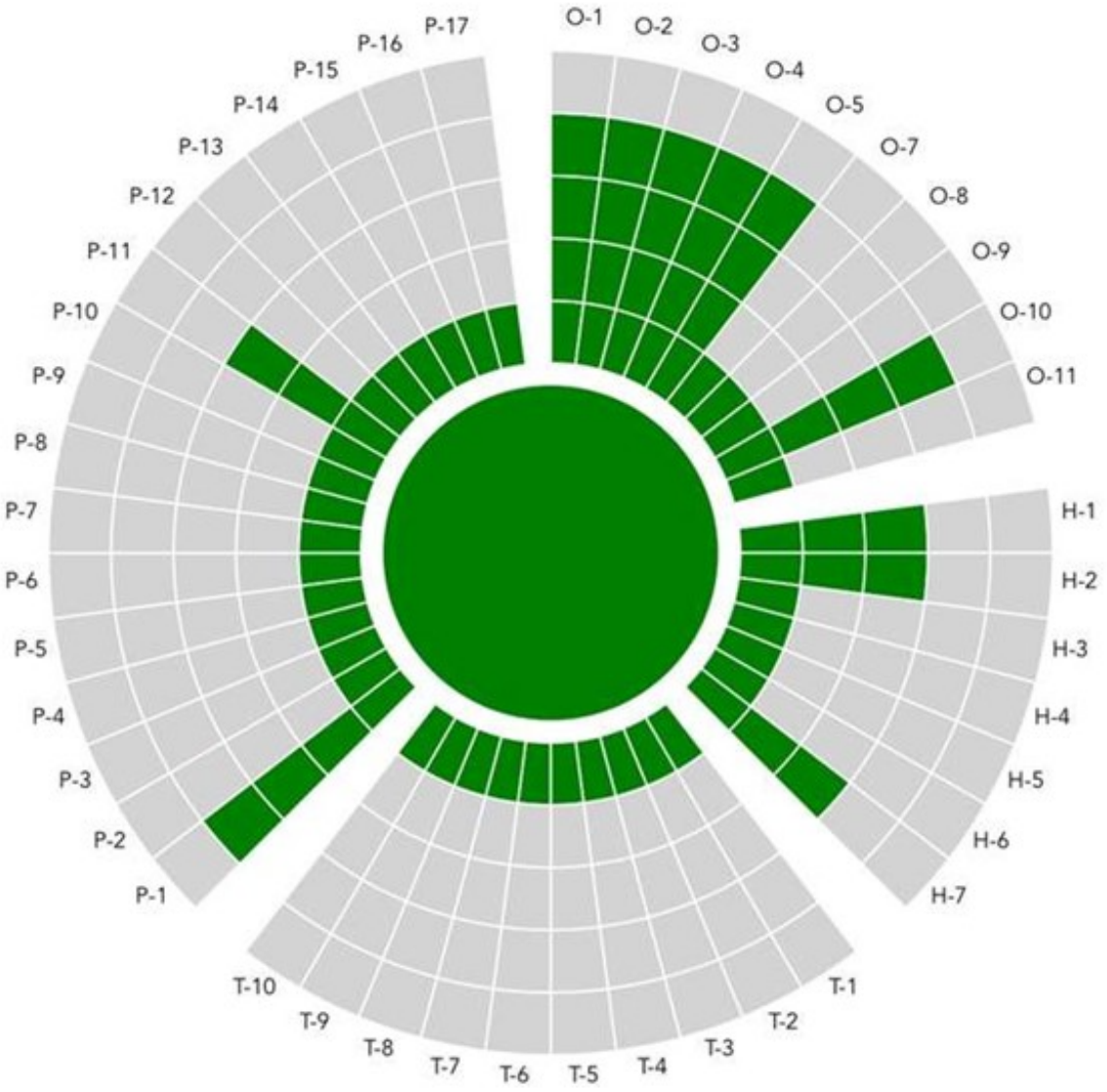
After the Site Visit the Primary Sponsor writes a Site Visit report which is part of the FIRST full member application process. This report must include the result of the assessment of the required subset of SIM3 parameters. The report is shared with the Secondary Sponsor and Candidate for comments and discussion.

7 - Sponsor to draft a Site Visit report
A sample template is available on Annex 7

Annex 3 – SIM3 Parameters

The following first table is derived from SIM3 and primarily targeted at cybersecurity incident management teams (CSIRTs, NCSCs, CDCs, CIRTs, etc.).

A second version of this table, but limited to only the 11 required parameters, and aimed at PSIRTs, and is further down in this Annex.



Parameter	Description	Required level
O – "Organization" Parameters		
O-1 MANDATE	Description: The CSIRT's assignment as derived from upper management.	3
O-2 CONSTITUENCY	Description: Who the CSIRT functions are aimed at CONSTITUENCY the "clients" of the CSIRT.	3
O-3 AUTHORITY	Description: What the CSIRT can do towards their constituency in order to accomplish their role.	3
O-4 RESPONSIBILITY	Description: What the CSIRT is expected to do towards their constituency in order to accomplish their role.	3
O-5 SERVICE DESCRIPTION	Description: Describes what the CSIRT service is and how to reach it. Minimum requirement: Contains the CSIRT contact information, service windows, concise description of the CSIRT services offered and the CSIRT's policy on information handling and disclosure.	3
O-7 SERVICE LEVEL DESCRIPTION	Description: Describes the level of service to be expected from the CSIRT. Minimum requirement: Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CSIRTs. For the latter a human reaction within two working days is the minimum expected.	-
O-8 INCIDENT CLASSIFICATION	Description: The availability and application of an incident classification scheme to recorded incidents. Incident classifications usually contain at least "types" of incidents or incident categories. However, they may also include the "severity" of incidents.	-
O-9 INTEGRATION IN EXISTING CSIRT SYSTEMS	Description: Describes the CSIRT's level of membership of a well-established CSIRT co-operation, either directly or through an "upstream" CSIRT of which it is a customer/client. This is necessary to participate and integrate in the trans-national/worldwide CSIRT system(s).	-
O-10 ORGANIZATIONAL FRAMEWORK	Description: Fits O-1 to O-9 together in a coherent framework document serving as the controlling document for the CSIRT. Minimum requirement: Describes the CSIRT's mission and parameters O-1 to O-9.	3

Parameter	Description	Required level
	note: for FIRST application, change "O-1 to O-9" into "O-1 to O-5"	
O-11 SECURITY POLICY	Description: Describes the security framework within which the CSIRT operates. This can be part of a bigger framework, or the CSIRT can have their own security policy.	-
H – "Human" Parameters		
H-1 CODE OF CONDUCT/ PRACTICE/ ETHICS	Description: A set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work. Clarification: E.g. the FIRST Code of Ethics. Behavior outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.	2
H-2 PERSONNEL RESILIENCE	Description: How CSIRT staffing is ensured during illness, holidays, people leaving, etc. Minimum requirement: three (part-time or full-time) CSIRT members.	2
H-3 SKILLSET DESCRIPTION	Description: Describes the skills needed on the CSIRT job(s).	-
H-4 INTERNAL TRAINING	Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones.	-
H-5 (EXTERNAL) TECHNICAL TRAINING	Description: Program to allow staff to get job-technical training externally – like FIRST training, TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.)	-
H-6 (EXTERNAL) COMMUNICATION TRAINING	Description: Program to allow staff to get (human) communication/presentation training externally.	-
H-7 EXTERNAL NETWORKING	Description: Going out and meeting other CSIRTs. Contributing to the CSIRT system when feasible.	2

Parameter	Description	Required level
T – "Tools" Parameters		
T-1 IT RESOURCES LIST	Description: Describes the hardware, software, etc. commonly used in the constituency, so that the CSIRT can provide targeted advice.	-
T-2 INFORMATION SOURCES LIST	Description: Where does the CSIRT get their vulnerability/threat/scanning information from.	-
T-3 CONSOLIDATED E-MAIL SYSTEM	Description: When all CSIRT mail is (at least) kept in one repository open to all CSIRT members, we speak of a consolidated e-mail system.	-
T-4 INCIDENT TRACKING SYSTEM	Description: A trouble ticket system or workflow software used by the CSIRT to register incidents and track their workflow. Clarification: RTIR, AIRT, OTRS, trouble ticket systems in general.	-
T-5 RESILIENT PHONE	Description: The phone system available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements. Clarification: Mobile phones are the easiest fallback mechanism for when a team's landlines are out of order. Minimum requirement: Fallback mechanism for the case of phone system outages.	-
T-6 RESILIENT E-MAIL	Description: The e-mail system available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.	-
T-7 RESILIENT INTERNET ACCESS	Description: The Internet access available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.	-
T-8 INCIDENT PREVENTION TOOLSET	Description: A collection of tools aimed at preventing incidents from happening in the constituency. The CSIRT operates or uses these tools or has access to the results generated by them. Clarification: e.g. IPS, virus scanning, spam filters, port scanning. If not applicable as for a purely coordinating CSIRT, choose -1 as Level and will be omitted from "scoring".	-

Parameter	Description	Required level
T-9 INCIDENT DETECTION TOOLSET	Description: A collection of tools aimed at detecting incidents when they happen or are near happening. The CSIRT operates or uses these tools or has access to the results generated by them. Clarification: e.g. IDS, Quarantine nets, NetFlow analysis.	-
T-10 INCIDENT RESOLUTION TOOLSET	Description: A collection of tools aimed at resolving incidents after they have happened. The CSIRT operates or uses these tools or has access to the results generated by them. Clarification: e.g. basic CSIRT tools including who is, traceroute etc.; forensic toolkits.	-
P – "Processes" Parameters		
P-1 ESCALATION TO GOVERNANCE LEVEL	Description: Process of escalation to upper management for CSIRTs who are a part of the same host organization as their constituency. For external constituencies: escalation to governance levels of constituents.	3
P-2 ESCALATION TO PRESS FUNCTION	Description: Process of escalation to the CSIRT's host organization's press office.	-
P-3 ESCALATION TO LEGAL FUNCTION	Description: Process of escalation to the CSIRT's host organization's legal office.	-
P-4 INCIDENT PREVENTION PROCESS	Description: Describes how the CSIRT prevents incidents, including the use of the related toolset. Also, this includes the adoption of proactive services like the issuing of threat/vulnerability/patch advisories.	-
P-5 INCIDENT DETECTION PROCESS	Description: Describes how the CSIRT detects incidents, including the use of the related toolset.	-
P-6 INCIDENT RESOLUTION PROCESS	Description: Describes how the CSIRT resolves incidents, including the use of the related toolset.	-
P-7 SPECIFIC INCIDENT PROCESSES	Description: Describes how the CSIRT handles specific incident categories, like phishing or copyright issues. Clarification: may be part of P-6.	-
P-8 AUDIT/FEEDBACK PROCESS	Description: Describes how the CSIRT assesses their setup and operations by self-assessment, external or internal assessment and a subsequent feedback mechanism. Those	-

Parameter	Description	Required level
	elements considered not up-to-standard by the CSIRT and their management are considered for future improvement.	
P-9 EMERGENCY REACHABILITY PROCESS	Description: Describes how to reach the CSIRT in cases of emergency. Clarification: Often only open to fellow teams.	-
P-10 BEST PRACTICE E-MAIL AND WEB PRESENCE	Description: Describes (1) the way in which generic, security related mailbox aliases @org.tld are handled by the CSIRT or by parties who know when what to report to the CSIRT – and (2) the web presence.	-
P-11 SECURE INFORMATION HANDLING PROCESS	Description: Describes how the CSIRT handles confidential incident reports and/or information. Also has bearing on local legal requirements. Clarification: it is advised that this process explicitly supports the use of TLP, the Traffic Light Protocol.	2
P-12 INFORMATION SOURCES PROCESS	Description: Describes how the CSIRT handles the various information sources available to the CSIRT (as defined in the related tool, if available – see T-2).	-
P-13 OUTREACH PROCESS	Description: Describes how the CSIRT reaches out to their constituency not in regard incidents but in regard PR and awareness raising.	-
P-14 REPORTING PROCESS	Description: Describes how the CSIRT reports to the management and/or the CISO of their host organization, i.e. internally.	-
P-15 STATISTICS PROCESS	Description: Describes what incident statistics, based on their incident classification (see O-8), the CSIRT discloses to their constituency and/or beyond. Clarification: If not applicable as in case of an explicit choice only to report internally, choose -1 as Level and will be omitted from "scoring".	-
P-16 MEETING PROCESS	Description: Defines the internal meeting process of the CSIRT.	-
P-17 PEER-TO-PEER PROCESS	Description: Describes how the CSIRT works together with peer CSIRTs and/or with their "upstream" CSIRT.	-

Below follows the PSIRT-tailored version of the above table. It is limited to only the 11 required parameters:

Parameter	Description	Required level
O – "Organization" Parameters		
O-1 MANDATE	Description: The PSIRT's assignment as derived from upper management..	3
O-2 CONSTITUENCY	Description: Who the PSIRT functions are aimed at CONSTITUENCY the "clients" of the CSIRT.	3
O-3 AUTHORITY	Description: What the PSIRT can do towards their constituency in order to accomplish their role.	3
O-4 RESPONSIBILITY	Description: What the PSIRT is expected to do towards their constituency in order to accomplish their role.	3
O-5 SERVICE DESCRIPTION	Description: Describes what the PSIRT service is and how to reach it. Minimum requirement: Contains the PSIRT contact information, service windows, concise description of the PSIRT services offered and the PSIRT's policy on information handling and disclosure.	3
O-10 ORGANIZATIONALFRAMEWORK	Description: Fits O-1 to O-9 together in a coherent framework document serving as the controlling document for the PSIRT. Minimum requirement: Describes the PSIRT's mission and parameters O-1 to O-9. ***note***: for FIRST application, change "O-1 to O-9" into "O-1 to O-5"	3
H – "Human" Parameters		
H-1 CODE OF CONDUCT / PRACTICE / ETHICS	Description: A set of rules or guidelines for the PSIRT members on how to behave professionally, potentially also outside work. Clarification: E.g. the FIRST Code of Ethics. Behavior outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.	2
H-2 PERSONNEL RESILIENCE	Description: How PSIRT staffing is ensured during illness, holidays, people leaving, etc.	2

Parameter	Description	Required level
	Minimum requirement: three (part-time or full-time) PSIRT members.	
H-7 EXTERNAL NETWORKING	Description: Going out and meeting other CSIRTs. Contributing to the CSIRT/PSIRT system when feasible.	2
P – "Processes" Parameters		
P-1 ESCALATION TO GOVERNANCE LEVEL	Description: Process of escalation to upper management for PSIRTs who are a part of the same host organization as their constituency. For external constituencies: escalation to governance levels of constituents.	3
P-11 SECURE INFORMATION HANDLING PROCESS	Description: Describes how the PSIRT handles confidential incident reports and/or information. Also has bearing on local legal requirements. Clarification: it is advised that this process explicitly supports the use of TLP, the Traffic Light Protocol.	2

Annex 4 – Sponsor Letter Template

The below text may be included in both Sponsor Letters, and as inspiration for such letters.

When completed, the Sponsor Letter(s) should be converted into a PDF format, on letterhead (recommended), signed and uploaded to the application on the portal. Primary and Secondary Sponsor each sign their own Sponsor Letter.

I [sponsor] attest that the Candidate satisfies the minimum requirements for FIRST membership.
I [sponsor] am familiar with the way the Candidate operates.
I [sponsor] have met the Candidate and presented FIRST and answered their questions.
I [sponsor] have had working interaction with the Candidate.
I [sponsor] have verified the required subset of SIM3 parameters with the Candidate and verified that they meet the mandatory score for those parameters.
I [sponsor] have explained the confidentiality of the information that is passed within FIRST and the Candidate agrees to comply with that. TLP and the FIRST Code of Ethics were also discussed.

I [sponsor] trust that the Candidate will be a good contributor to the FIRST vision and mission.

Any other comments/recommendations:

Sponsor (team name)
Sponsor (contact name)
Title/function
Date
Signature

Annex 5 - Terms and Definitions

- **Candidate** – The Team that wishes to become a full member of FIRST, and benefits from the sponsorship.
- **Sponsors** – FIRST full members in good standing, who assist (sponsor) a Candidate in becoming a FIRST team member. Two Sponsors are needed for the membership process. Only Teams can sponsor a candidate, Liaisons cannot. However, for practical reasons, for each Sponsor, one of the team representatives will formally validate the proceedings.
- **Site Visit** – The visit that one of the Sponsors makes to the candidate's premises, with the goal of verifying if the candidate meets the FIRST membership requirements. In special cases, and only with explicit permission by FIRST, the Site Visit can be performed virtually instead of live, using videoconferencing tools (audio only is not permissible).
- **SIM3** –"Security Incident Management Maturity Model". CSIRT Maturity is an indication of how well a team governs, documents, performs, and measures their function. The maturity of a CSIRT is measured with SIM3.
- **Primary Sponsor** – The Sponsor that performs the Site Visit and writes the report about it.
- **Secondary Sponsor** – The additional Sponsor that supports both the Candidate and the Primary Sponsor.
- **FIRST Secretariat Services (FSS)** – The FIRST secretariat receives the documents sent by the Candidate, validates them, and requests updates in case of discrepancies. Then it updates the FIRST portal, uploads the documents, and fills in the monthly "Membership Applications Status Report" to be sent to the FIRST Membership Committee for pre-validation. Once achieved, FIRST secretariat sends the applications to the FIRST Board and after validation, disseminate the new member to the FIRST community members.
- **FIRST Membership Committee (MC)** – Standing committee that advises FIRST on all matters related to the FIRST Membership. The MC consists of volunteers from the ranks of FIRST full and liaison members. The MC reviews membership applications, and can recommend acceptance, or ask for more information/validations, or recommend rejecting the application.
- **Mentor** – An MC member who helps Sponsors and Candidate throughout the process. Mentors are appointed by the FIRST Secretariat only in cases of perceived need for mentoring.

- **FIRST Board of Directors (BoD)** – The Board of Directors of FIRST. Elected by the members, the Board is the highest decision-making body of FIRST.
- **Team Representative** – A Candidate team member who will act as Representative for the Candidate team. Short name is "Team Rep". Two Team Representatives are required for each team: The "Primary Team Rep", and the "Secondary Team Rep". The Team Representative's role is to represent the whole team, especially during the Annual General Meetings (AGM) of FIRST. The Team Representative does not need to have a formal management position inside the Candidate team, it is up to the Candidate to name a proper Team Rep. However, the Team Rep should either be a member of the Team, or of the hierarchy that governs the Team.

Annex 6 – Version History

1. Version history

This document was originally produced by the CERT Program at the Software Engineering Institute at Carnegie Mellon University and by the Cisco Systems PSIRT

- April 13, 2006 - Robin Ruefle (CERT Program), Damir Rajnovic (PSIRT) o First public release as "FIRST Site Visit"
- August 2013 - Margrete Raaum (UiO-CERT), Robin Ruefle (CERT/CC)
- January 2019 – Alexander Jaeger (BASFgCERT), Mike Murray, Rohit Srivastwa, Martijn van der Heide (MC members)
- November 2019 - Andrea Dufkova (ENISA), MC members
- December 2020 – Andrea Dufkova, Olivier Caleff, Baiba Kaskina and Don Stikvoort (MC members) and reviewed by all MC Committee members
    - Renamed to "FIRST Membership Sponsoring Process"
    - Added SIM3 reference model as the basis for the Site Visit
    - Added the role of a Mentor as a support
    - Made explicit the reapplication process in case of a rejection of the application
- April 2021 - FIRST Membership Sponsoring Process, version 2.0
- July 2023 - Renamed to *FIRST Membership Process*, version 2.1

Annex 7 – Site Visit Report Template

Please note, this is a sample template for a site visit report. The sponsors can modify as needed or note if any sections of the template or not applicable to the applying team and why.

[Candidate]
SITE VISIT REPORT

[Date of Visit]

Sponsored by
[Primary Sponsor]
[Primary Sponsor Contact and Email]

INDEX

- Cooperation with other teams
- Any other policies

Workplace and environment
- Physical security and facilities
- Equipment
- Storage
- Incident creation/tracking
- Network infrastructure
- Use of PGP

Incident Handling
- How to report an incident
- Incidents can be reported by email
- Incident handling process
- Acknowledging report (option, but recommended)

Contact information and information dissemination
- Internal vs external

Professional development
- Training
- Conferences
- Remote Visit (if applicable)

Signatures

Sponsoring Team Representative **[Primary Sponsor Contact]** visited **[Candidate]** on **[Date of Visit]** **[in-person at [Location]|virtually]**. The following individuals **[Candidate Contacts]** were present. During the site visit, the incident handling and security procedures were reviewed. The team also reviewed examples of past incidents that they experienced with customers and/or projects.

General items

Team information is available at **[URL of public Candidate information]** and in the RFC 2350 format provided in the application documentation.

Defined Constituency

[Please include a detailed description of your constituency]

The CSIRT's constituency is defined as the 'client base', the target group for whom you do the CSIRT work. This constituency can be your own organization or company - then it is said that your constituency is internal to your organization. Your team can also have a constituency external to your own organization, like for instance your country's universities

when you serve the academic community, or a paying customer base (commercial), or all municipalities in your country.]

Mission statement or charter

[Include mission statement, I=insert URL if mission statement is published]

Example: *"**[Candidate]** is aimed to provide a reliable and trusted single point of contact for an effective incident response related to technology and ICTs (Information and Communications Technologies) into the financial sector and critical infrastructures in the public and private sector."*

Document of creation, effective start date and announce

[Candidate] has started to operate **[month/year of establishment]** and they have established cooperation with several teams such as **[insert team names]**.

Defined and advertised set of services provided for the constituency?

Their service portfolio is listed at **[insert link]**, they provide the following services.

Refer to the application/list of services base on the CSIRT/PSIRT Framework.

Funding models in place

TEAM is funded by a **[Parent Organization/Host]** (**[insert url]**) in **[country]** and specializes in providing **[example: *IT and consulting*]** services.

Organizational Home

[Contact information is listed here (ex: *cert.organization.url/contact/*)]

Policies

Members of **[Candidate]** must sign a written statement regarding the usage of information, systems and resources. They are currently in the process of implementing ISO 27001 policies, and most of this information is covered in the internal policies reviewed during the site visit.

Information classification

Addressed in the TEAM internal policy x

Information protection

Addressed in the TEAM internal policy x

Record Retention

Addressed in the TEAM internal policy x

Record destruction

Addressed in the TEAM internal policy x

Information dissemination

Addressed in the TEAM internal policy x

Access to information

Addressed in the TEAM internal policy x

Appropriate usage of systems

Addressed in the TEAM internal policy x

Computer security events and incidents definition

Incident handling policy

Cooperation with other teams

[Candidate] has been collaborating with other FIRST Teams members, such as **[team names]**, and have contacts with government teams in **[country/industry]** and will support the development of other incident response teams in the region.

Any other policies

[Insert any other policies here]

Workplace and environment

Physical security and facilities

Example: *To access the **[Candidate]** building a legal photo ID (passport, national identity card, etc) is **[required/requested]**. The **[Candidate]** facilities are physically separated from the rest of the organization. To enter team facilities the process is **[insert process]**. Access to the servers and network infrastructure is also restricted, and only authorized members can access these facilities.*

Equipment

Example: ***[Candidate]** members have **[number]** computers, one connected to the internal network, and another connected to the CSIRT network which is isolated from the rest of the organization network. Some users also have access to connect to test networks. **[Candidate]** systems are managed internally by the CSIRT system administrators and systems are kept updated and backups are performed daily.*

Storage

Example: ***[Candidate]** infrastructure has several storage facilities isolated from the other parts of the organization that are used for backup and storage.*

Incident creation/tracking

Example: *The team uses **[description of tools]** for tracking incidents and also to implement the different live ISO 27001 procedures.*

Network infrastructure

Example: ***[Candidate]** network is isolated from the organization network, with different internet connections. They have other networks also for testing purposes.*

Incident Handling

How to report an incident

Example: *External users can use the information provided in **[link to documentation - example /cert.organiation.url/report-incident/]**. Clients also have a support desk that can be accessed **[describe]**.*

Incidents can be reported by email

Yes, also by telephone and postal address that are noted in the application form.

Incident handling process

Example: *Most alerts came directly from their clients as a result of an alert generated in their systems that are handled by **[Candidate]** members. End users can also contact them by email or by use of specific forums in which they help them to fix the problems.*

Acknowledging report (optional, but recommended)

Describe how incidents are added to the database and acknowledged/responded to by email, tracked, coordinated and reported.

Contact information and information dissemination

Internal vs external

Example: *Internally, **[Candidate]** uses different systems to store and disseminate information, such as **[wiki/ticketing tool]** for tracking incidents.*

For clients, TEAM has various portals that they can use to contact the team. Information to the public includes listing of free security tools, statistics of virus dissemination and documentation about incident recovery.

Professional development

Training

Example: ***[Candidate]** members have attended the following courses and also have attended events/conferences such as **[list]**. **[Candidate]** members have several certifications in computer security including **[list]**.*

Conferences/Special Interest Groups

[Candidate] is willing to participate in the following FIRST conferences/meetings/SIGs **[list]**

Remote Visit (if applicable)

Insert pictures/screenshots or other details from the remote visit

Signatures

_____	_____
Sponsoring Team Representative	Applying Team Representative
Team Name	Team Name
Date	Date

Annex 8 - Application Process Steps, Stakeholders and estimated duration

A high-level view on the process with the steps, stakeholders, and estimated duration is presented below:

M Mandatory | R Recipient | (o) Optional

	Steps	Candidate	Primary Sponsor	Secondary Sponsor	FIRST Secretariat	FIRST MC	Mentor	FIRST Board	FIRST Community	Estimated Duration	
A team wishes to become a FIRST Full Member and completes the *Membership Interest Form*	1	M									
Candidate must find two FIRST full members who agree to act as Sponsors	2	M	M	M	(o)	(o)	(o)			1m	*Estimated duration: 5 months*
Candidate schedules the site visit with their primary sponsor	3	M	(o)	(o)						1w	
Candidate performs a SIM3 self-assessment	4	M					(o)			1w	
Primary Sponsor conducts Site Visit	5	M	M	(o)						1d	
Candidate completes the *Full Member Application Form*	6	M	(o)	(o)			(o)			1m	
Sponsors review candidacy	7		M	(o)						1w	
Sponsors write supporting letters and Site Visit report	8		M	M						1w	
All materials are submitted for review	9	M			R		(o)			1d	
Candidacy compliance check by the FIRST Secretariat	10				M					1m	
Membership Committee review	11					M				2w	
Review by Membership and Board	12							M	(o)	2w	
Application feedback and reapplication (if needed)	13	(o)	(o)	(o)	(o)					2m	
FIRST Board votes on application	14							M		1m	
Notification	15	M	M	M	M				R	1w	