FIRST Site Visit Requirements and Assessment

Document originally produced by CERT Program at the Software Engineering Institute at Carnegie Mellon University and Cisco Systems PSIRT.

REVISION	WHEN	WHO
1.0	April 13, 2006	Robin Ruefle (CERT Program), Damir Rajnovic (PSIRT)
2.0	August 2013	Margrete Raaum (UiO-CERT), Robin Ruefle (CERT/CC)
3.0	December 2014	Margrete Raaum (Statnett SF)
3.1	May 2020	Andrea Dufkova

FIRST Site Visit Documents Overview

As part of acquiring FIRST membership, a team must host a site visit from an appointed FIRST team, one of their sponsors. This site visit is to ensure that the candidate CSIRT meets all needed requirements to be an active and beneficial member of FIRST. It is also to ensure that information and data shared by FIRST will be appropriately handled and protected.

The detailed process of becoming a FIRST member is described at https://www.first.org/membership/.

The items in this site visit evaluation document are suggestions to applying teams and sponsors of what to review during the site visit and what to look for as a way to assess of the qualifications of the candidate team. Not all questions/categories may apply to every team. We have also added a checklist with areas to comment on the last two pages for reporting purposes.

What is a site visit and why is it done?

The purpose of the site visit is to verify that the applying team satisfies the requirements for FIRST membership. The primary reason is to protect the confidentiality of the information that is passed within FIRST. The secondary reason is to

familiarize the visiting team (sponsor) with the way the candidate team operates. Lastly, this it is an opportunity to meet candidate's teams' managers, present FIRST as an organization and answer any questions the candidate team might have.

Will site visit make the candidate trusted?

The site visit will not make a candidate team trusted by other members of FIRST or make the candidate team trust other FIRST member teams. The visit is to provide assurance that critical operational and managerial issues are up to a certain standard and that some minimum requirements are met. Trust may develop with time and through interaction with other teams.

The candidate and the sponsor will act in good faith. The sponsor's role is to establish facts and answer questions but not to investigate or judge.

Providing documentary evidence

The sponsor will ask for some documentary evidence related to the candidate. We suggest that the sponsor and the candidate team discuss documents that will be requested in advance. This gives, the candidate time to provide the requested documents before the site visit. If the documents exist, but for some reason cannot be produced, the candidate should state so and provide as much detail verbally as possible. The sponsor must note which documents were not available and the reasons why in the site visit checklist. An overview of the reviewed or the unavailable documents should be noted in the final report.

How to do site visits for distributed teams?

If the candidate team is distributed over more than one physical location, the sponsor must visit at least one site that is mutually agreed upon. It does not have to be the 'main' site. If the other sites are at a different standard as the visited site, the sponsor must note and detail differences.

What happens after the site visit?

After the site visit, the sponsor submits its findings in a report to the FIRST secretariat. The secretariat submits the membership package to the FIRST Membership Committee, to the FIRST membership, and finally to the FIRST steering committee for review. At any stage additional questions can be raised and it is the sponsor's duty to address them.

Application pass/fail criteria

If a question is raised any time during the application validation, and the sponsor, with the help of the candidate, cannot satisfactory address it, the application will fail. To

assess an item in the Site Visit Document as satisfactory means that the candidate team has either fully complied with the requirement(s) or provided sound reasons why the item is not applicable to them. The FIRST Steering Committee has the discretion to intervene and accept candidates into membership irrespectively of the site visit results.

If the candidate team passes the site visit are they a member of FIRST?

No, the site visit is only a component of the application process. The information collected during the visit will be posted for FIRST members to review. If there are no objections after the candidate has been reviewed by the FIRST membership, the application will go to the FIRST Steering Committee for approval.

Not all questions are relevant to a particular site visit

The site visit document was created to fit a profile of a generic team. Not all questions will be applicable to all teams. All such instances must be documented together with the reasons why they are not applicable.

How should the site visit report be submitted?

After each item the sponsor may summarize the findings. If a checklist is included for a particular bullet then the appropriate box must be ticked by putting an 'x' in it. Any caveats, deliberations, thoughts and comments must be noted. Information should be collected in a single file and sent to FIRST Secretariat as a PDF document in a secure electronic format, signed by the sponsor. The notes can be either typed in a document or written on a piece of paper and then scanned.

Suggested Course of Action

Candidates are recommended to review their status against the site visit document prior to the sponsor site visit. If issue are identified the candidate can resolve prior to the site visit. If the review confirms that the candidate meets all requirements then the formal application can be submitted in an expedited manner.

FIRST Site Visit Evaluation Document

This document presents the CSIRT requirements that will be reviewed at the site visit. This list of requirements is inspired by the previous work done by the CERT Program at the Software Engineering Institute at Carnegie Mellon University and other accreditation programs like the Trusted Introducer Program. The purpose is to evaluate the level of readiness of a candidate for FIRST membership. The list is not exhaustive and it should be expanded with additional items depending on the candidate's circumstances.

All mandatory items are marked with the word "Mandatory". Items not marked are considered optional.

1. General items

1.1. Defined constituency (Mandatory)

For a CSIRT, understanding the constituency will help the team determine what needs they have, what type of assets they protect, and what kind of interaction there will be with the team.

Each team must have a clearly defined constituency. If there is overlap with any other team, this must be made known, and the constituency know when to engage which of the teams.

Verification of the constituency can be found in any charters, mission statements, concept of operations documents, or similar documents that describe the CSIRT's purpose and function.

As part of completing this requirement, the type of constituency and sector should be recorded as "Constituency type" and "Constituency sector", where "type" could be: internal, external or mixed, and "sector" could be: educational, government, non-profit, critical infrastructure, military, commercial or other.

1.2. Mission statement or charter (Mandatory)

As outlined in RFC 2350, the mission should be documented, and should explain the purpose and function of the CSIRT in a clear manner. It should list a brief overview of the core goals and objectives of the team.

1.3. Document of creation, effective start date, and announcement (Mandatory)

This is a formal document by which the CSIRT is established. It outlines its approved operations and authority and notes the effective start date the team went into operation. This could be a memo from executive management or some other similar document. This could also be part of the mission and charter in item 1.2.

The effective start date that the team went into operation should be recorded. This is the date on which the team has officially started its existence. This can be included as part of the Document of Creation discussed in item 1.5 or other documents.

The CSIRT's existence must be announced to the constituency. When a CSIRT becomes operational there should be an announcement to its constituency declaring it so and describing the interface with the constituency. They must know that it is exists and know how to engage and interact with the CSIRT.

If the constituency is internal, then the announcement should be made internally. If desired and appropriate the announcement can be made externally too. If the constituency is external, then the announcement should be made externally.

This can be verified by reviewing the actual announcement and any subsequent descriptions such as a web page or charter.

1.4. Defined and advertised set of services provided for the constituency (Mandatory)

A defined set of services should explain what actions, functions, or deliverables it performs for the constituency. It should also include any service level definitions that have been agreed to between the CSIRT and the constituency.

Verification of a set or list of services should be accessible to the constituency via a brochure, website, or other similar mechanism.

1.5. A Funding model is in place (Mandatory)

To ensure long-term stability the CSIRT requires a funding model to be in place which provides incoming funds to ensure continued operation of the team and continued provision of CSIRT services to the constituency.

Funding for long-term operational, personnel, and facilities costs needs to be in place. The funding model can be for example:

A. a cost centre within an organization (where the host or parent covers all expenses and does not receive any revenue from it) or

B. team can be funded in whole or in part by grants, if so:

- who will give grants?
- what is the purpose of the grant?
- how much will the grants be for and how much of the operations will they cover?
- how secure is the funding source?
- how long is the grant in place?

The team should detail the grant include issuer and source, purpose, amount and duration of the grant.

C. Or the team may sell its service either internally or externally (there could be a charge-back or fee to internal or external customers.) or

D. be funded through a consortium of organizations such as universities in a research network

This can be verified by reviewing a copy of an accepted and approved budget or other financial documentation from the funding source.

1.6. Organizational Home (Mandatory)

The organizational home of the CSIRT indicates the team's position within the parent organization or constituency. An internal CSIRT could be located in its own or a larger department Many national teams are located in government organizations, while others may be associated with a research network or university.

The organizational home of a CSIRT can be verified by looking at an organization chart or diagram, or by looking at any announcement from management.

1.7. Team's organization (Operational)

The team's organization details the CSIRT staff members and leadership, their roles and responsibilities, and their corresponding location in the parent organization or constituency. The team structure can for example be virtual representing a broad part of an organization, a department in a larger organization or even a set standalone organization in itself.

The team's organization can be verified by looking at a CSIRT organization chart or similar document.

2. Policies

This section reviews various policies the CSIRT should have in place to ensure that incident data, vulnerability information, malware/artifacts and site information is properly protected. All of these policies should be verifiable by reviewing the policy document, along with any corresponding procedures. Verification can also be done by interviewing staff to see if they know and understand the policies.

2.1. Information classification (Mandatory)

This policy should detail the CSIRT's categorization or classification of information, including distinctions between sensitive, confidential or public information.

These classifications should apply to information in any form; electronic or hardcopy.

The policy should specify how to categorize any information received from FIRST teams.

2.2. Information protection (Mandatory)

This policy should describe how differently classified information is protected in storage, transit, access etc. It should include what type of information must stay within the CSIRT facility and how information should be handled on laptops and other mobile devices. It should also detail what type of information can and cannot be discussed on mobile or non-secure devices along with what information must be transmitted and discussed and stored in a secure fashion and should not be shared or discussed with non-authorized persons.

This policy should also state the manner in which FIRST information should be handled, protected, and shared within the CSIRT and its parent/host organization.

2.3. Record retentions (Mandatory)

This policy should detail how long various classifications of information are retained and stored by the CSIRT It should also detail how the generations of information is stored and protected, including how backups are handled, transported, and archived.

2.4. Record destruction (Mandatory)

This policy should detail how information (electronic and hardcopy) is destroyed, based on its classification. This should detail how media such as hard drives, portable storage devices etc. are destroyed. It should also discuss how hardcopies of information are shredded and by whom.

The policy should specify that any information that is sensitive, site-related, or confidential should be destroyed only by those with approved access and must be destroyed in a manner that it cannot be reconstituted.

2.5. Information dissemination (Mandatory)

All CSIRT staff require information disclosure guidelines to know what they can say and to whom they can say it. Constituents also need to know what level of confidentiality they can expect when they report incident activity or attacks to the CSIRT.

This policy should discuss the type of information that can be disseminated to internal and external groups the methods by which information should be disseminated (including how information from FIRST coming into the CSIRT will be shared), the specific types of information that will not be released and what information should be considered sensitive or confidential.

This policy should take into account the information disclosure restrictions that might be placed on information provided to a CSIRT by other organizations and the parent organization, which might have its own requirements (For example, if another CSIRT reports an incident, what can its constituents expect regarding the disclosure of the information reported? The policy should specify limitations, which should be made publicly available (to the constituents and other interested parties such as law enforcement).

2.6. Access to information (Mandatory)

This policy should highlight what type and classification of information can be viewed or accessed by members of the CSIRT staff, staff from the parent or host organization, members of the constituency, and any external parties. There may be different levels of information, particularly sensitive or confidential information that will require a higher level of authorization for access.

It should also detail who has the authority to change access and who has responsibility for maintaining the access process.

2.7. Appropriate usage of CSIRT's system (Mandatory)

This is an acceptable use policy that details how CSIRT staff should use CSIRT equipment and systems in their day to day operations.

This policy and corresponding procedures should outline the appropriate use of systems, e.g.

- How is the team equipment secured against unauthorized access?
- Can systems be used for personal activities?
- What sites can and cannot be connected to from CSIRT systems?
- Can personal software can be downloaded and installed on CSIRT systems?
- how often and what type of backups are made of data on CSIRT systems
- required security configurations for software, including browsers
- what type of virus and spyware scanning is done and how often
- how software updates and patches are installed
- the proper method of accessing remote CSIRT services and systems remotely

This policy can also list disciplinary actions to be taken if the policy is not followed.

2.8. Computer Security Events and Incidents Definition (Mandatory)

There must be some criteria against which a report can be evaluated, to determine if it is an incident and to categorize it.

- what is the definition of computer security incident for the CSIRT and constituency
- what criteria is used to evaluate event and incident reports
- what incident categories and corresponding priorities exist
- how are reports, events, and incidents correlated and combined

2.9. Incident handling policy (Mandatory)

The incident handling policy should define who has responsibility for handling what type of computer security incidents and who can be called in to assist in the response implementation from other areas.

This includes

- the types of incidents that fall within the jurisdiction or expertise of the CSIRT
- who handles the analysis and response
- what work, if any, should be done with law enforcement
- what to do with reports and activity outside the scope of the CSIRT

This policy should outline the basic process to follow in handling an incident. It should include:

- timeframes for response
- methods for escalation
- procedures for information and communication
- how incidents are tracked and recorded

- when and how incidents are closed
- how additional assistance is procured for analysis or for implementing suggested mitigation and recovery strategies.

2.10. Cooperation with other teams (Mandatory)

This policy should define the process followed by the CSIRT to engage in formal or informal cooperation with other teams. It should outline what type of agreements, NDAs, and SLAs are required and what type of information can be exchanged.

If teams in a cooperative forum (e.g., ISACs, FIRST) have a competitive relationship, specific guidance should be given as to what data can be appropriately shared and if there are any other special provisions for how the interaction should be handled.

2.11. Any other policies

Any other policies that the CSIRT has created or that the parent/host organization has established that affect the operation of the CSIRT or its membership in FIRST should be reviewed.

3. Workplace and environment

To perform work efficiently and effectively, a team needs to have the right workplace, environment and infrastructure in place.

All locations (if there are several locations) should provide the same, or equivalent, level of privacy and protection.

The site visit team should verify that the facilities/premise occupied by the CSIRT meets the minimal security standards as listed in the following sections. This can be done by observation or by reviewing descriptive documentation or blue prints. If this information is confidential, then it must be described as much as possible by the CSIRT.

The site visit team should also make sure that all equipment, networks, and applications are used in a manner to protect CSIRT data.

3.1. Physical security and facilities (Mandatory)

CSIRT facilities and network and telecommunications infrastructure must be designed with great care to not only protect the sensitive data collected by the CSIRT but also to protect the CSIRT staff. Information and staff areas should be built and protected in the same manner and meeting the same requirements as a data center.

Notable physical security considerations can include e.g.:

- secured rooms or security operations center (SOC) for location of any CSIRT servers and data repositories
- secured and sound proof rooms for discussion of CSIRT activities and investigations
- safe for storage of non-electronic data and notes
- secured communications mechanisms such as secure phones, faxes, and email
- physical separation of CSIRT staff from other parts of the organization
- policy on accommodating visitors if not included in policy on general access control

3.2. Equipment (Mandatory)

Make a note that the team has normal access to computers, phones, shredders and other relevant equipment.

3.3. Storage (Mandatory)

Each team will have material to store. The material can vary from papers, books, tapes, CDs, hard drives, computers and other equipment (or parts of it). Stored material can differ in its classification (books shared within the team vs. confidential data on an investigation) and purpose (unused items waiting for destruction vs. just currently unused items).

- Issues to be reviewed by the FIRST site visit:
- Where is the storage? Is it remote or on-site?
- What is being stored there?
- Who has access to it?
- Is there any audit trail on what is being put in, when and by whom?
- The same for taking items out of the storage.
- Is the storage fit for the purpose?
- How will FIRST data be stored?

FIRST site visit reviewers should look to ensure that information is appropriately protected and guarded against unauthorized access, accidental destruction, and disasters.

3.4. Incident creation/tracking (Mandatory)

Incidents must be tracked. The tracking system should include safeguards from unauthorized usage and must have audit capabilities so that it is possible to determine, who was using it and during what time period.

Any incident tracking system that is used by the CSIRT should be understood by the FIRST site visit team, since FIRST data may go in this tracking system. Specifically the following issues should be described, if not evident from the tracking system used:

- How will FIRST information be incorporated into this tracking system?
- Who has access to the tracking system? This will be particularly important if a group outside the CSIRT, such as a centralized helpdesk, has access to this tracking system. Is the CSIRT queue properly separated from the rest?
- At what point in a report's life is an incident created?
- How is it uniquely identified? Is there any unique tracking number?
- What is the format of that tracking number? What is the rationale for choosing this particular format over some other?
- If incidents are grouped or linked, how is that done? Is it assigned another tracking number or just added an attribute?
- How is the status of an incident demarcated (i.e., ongoing, closed, etc.)
- How is an incident closed? Where is it stored once closed?

3.5. Network infrastructure

Separate CSIRT LAN (Optional but recommended)

The team should have a separate LAN from the rest of the company. Network separation being either physical or logical.

Test network (Mandatory if applicable)

A test network is mandatory for testing unknown software (if the team does not do any software testing or malware analysis teams this is not applicable). Testing must not be done on a production network. Using a production machine for testing, even on virtual machines like VMware, should be discouraged. Ideally, the test network must be physically or logically separated from any other existing network, it may even have its own access to the Internet. There should be a policy in place that states the requirements for CSIRT staff when testing any malware or other programs on CSIRT systems. This policy should define where and how software and malware should be tested.

Infrastructure operations (Mandatory)

It should be established who operates team's network infrastructure, e.g. DNS, email, directory and Web servers, computers, data backup and handling backup media etc. The purpose is to identify possible weak spots where unauthorized information leakage can occur.

Usage of Secure Communications (Mandatory)

The site visit team should review what type of secure communications is used within the team, including requirements for using for secure communications.

3.6. Use of PGP (Optional)

Since PGP or GPG is recommended for communications in the FIRST community, how PGP is used in the team environment should be reviewed by the site visit team. Encryption keys must be distributed to all parties that will use it.

Questions about PGP should cover whether in addition to the team key, all have their individual keys and general key policies cound include e.g.

- who should have keys (staff, team, etc.)
- how keys will be created, managed, and archived.
- key management issues such as
- who will create the keys
    - what type of key should be created
    - what size key should be created
    - when will keys expire
    - if a revocation key is required
    - where keys and revocations will be stored
    - how keys will be revoked
    - who needs to sign a key
    - any password policies including password escrow
    - who manages the keys and corresponding policies and procedures for key management

4. Incident handling

The site visit team should review methods, processes, and technologies used by the CSIRT to handle incidents to ensure formalized procedures are in place that protect CSIRT data and allow efficient incident handling.

4.1. How to report an incident (Mandatory)

In order to handle a computer security incident the team must have a method of finding out about events and incidents. The constituency must have ways to communicate with the team to ask questions, report events and incidents, and receive feedback and guidance. This should be documented in the Incident Reporting Guidelines.

Incident reporting guidelines are written for the constituency and should outline the type of incidents that should be reported and the manner in which they should be reported.

Incident reporting guidelines can include

- the definition of an incident for your constituency
- an explanation for why an individual or group should report incident
- what kind of activity that can indicate an incident
- the identification of who or where the report should be sent
- an explanation of how to report
- a description of what should be included in a report
- an explanation of when to report

The guidelines can be used to explain

- who should receive the reports: the CSIRT directly, a centralized helpdesk, or some other group
- the exact method and procedures for submitting the information: via a form, via email, via phone calls
- the fields of information to be captured such as
    - contact information
    - time and date of report (including time zone information)
    - timeframe and date of activity
    - systems affected [OS version, patch level, purpose]
    - brief description of problem or activity
- any time requirements for submitting reports
- any other specifics for the CSIRT

4.2. Incident Response Plan (Mandatory)

The process by which the team receives and responds to computer security incidents should be reviewed by the site visit team. This should cover how incidents are

- Assigned
- Analyzed
- Escalated
- Closed
- Reviewed for lessons learned

Questions to be asked may include:

- Who records and tracks information about the incident?
- Is there any audit trail of actions taken, or how the incident has been updated?
- Are there any escalation procedures and corresponding process to raise the incident's priority?
- What kind of criteria are used to determine when an incident is closed?

4.3. Acknowledging report (Optional but recommended)

How a team acknowledges reports will be defined in any Service Level Agreements (SLAs) between the team and its constituency.

Questions to be asked by the site team may include:

- Within what time a message must be acknowledged?
- If team does not operate 24x7 how does it handle incoming messages out of working hours?
- Who receives incoming messages? Are they visible to whole team or not? Are they automatically archived? How?
- Will the incoming message be tagged somehow? How? At this stage we may not know if the report will become an incident or not but the information needs to be tracked. How it is done?

5. Contact information and information dissemination

5.1. Internal vs. external (where applicable)

Constituents need to understand how to contact and interact with the CSIRTs. A team's contact information should be advertised internally and externally as appropriate

This may be verified by reviewing any published contact information in brochures, employee handbooks, web sites or other similar communications.

Questions include:

Is there publicly advertised contact information? What is it? Including any URLs or email addresses or phone numbers.

- How is information disseminated?
    - Web?
    - Social media?
    - Email?

- Telephone?
- RSS, blogs etc.

6. Professional development Planning (Mandatory)

6.1. Training (Mandatory)

Incident Management is a dynamic field. To be effective team members must constantly acquire newknowledge.

- Are staff given time and resources to attend conferences and training?
- How is training tracked and regulated?
- Do job descriptions list required skills and abilities?
- Is there a professional development program?

6.2. Conferences (Mandatory)

Attending conferences is vital to acquire new knowledge and to make connections with other teams and individuals. To be considered an active team, someone from the team should attend at least one CSIRT-related event or conference a year. Please ask whether any other conferences are attended regularly, including the process for selection of conferences and team members that attend.

FIRST Site Visit Checklist and Acknowledgement

This checklist is based on FIRST Site Visit Requirements and Assessment document. (https://www.first.org/membership/site-visit-v3.1.pdf). The detailed process of becoming a FIRST member is described at https://www.first.org/membership/

The Primary Sponsor may acknowledge the following items were reviewed with the applying team during the site visit and their response meets FIRST standards.

1. General items

_____ We have reviewed the following items with the applying team.

1.1. Defined constituency

1.2. Mission statement or charter

1.3. Document of creation, effective start date, and announcement

1.4. Defined and advertised set of services provided for the constituency?

1.5. A Funding model is in place

1.6. Organizational Home

1.7. How the team is organized with the parent organization

Comments:

2. Policies

_____ We have reviewed the following policies the CSIRT should have in place to ensure incident, vulnerability, artifact, and site information is protected and secured. All of these policies can be verified by reviewing the policy document in writing, along with any corresponding procedures including:

2.1. Information classification

2.2. Information protection

2.3. Record retentions

2.4. Record destruction

2.5. Information dissemination

2.6. Access to information

2.7. Appropriate usage of CSIRT's system

2.8. Computer Security Events and Incidents Definition

2.9. Incident handling policy

2.10. Cooperation with other teams

Comments:

3. Workplace and environment

_____ The applying team has the right infrastructure in place that includes the CSIRT workplace, environment, and infrastructure includes physical location and security of CSIRT staff and data staff office and home equipment CSIRT networks, systems, and internal/external defenses such as routers, firewalls, and IDS CSIRT tools and applications to support incident handling and provided services such as (please describe in the comments section if virtual site visit):

3.1. Physical security and facilities

3.2. Equipment

3.3. Storage

3.4. Incident creation/tracking

3.5. Network infrastructure

3.6. Use of PGP or Identity Management Technology

Comments:

4. Incident handling

_____ We have reviewed the methods, processes, and technologies used by the CSIRT to handle incidents. We have ensured formalized procedures are in place that protect CSIRT data and allow efficient incident handling including:

4.1. How to report an incident

4.2. Incident Handling Process

4.3. Acknowledging report

Comments:

5. Contact information and information dissemination

_____ We acknowledge that:

5.1. Internal vs. external contact information is available

Comments:

6. Professional development

_____ The applying team participates in ongoing training.

6.1. Training

6.2. Conferences

Comments:

7. Virtual Site Visit

We acknowledge:

_____ A physical site visit was not possible at this time but I have met with the team/members of the team in person on other occasions (recommended). Please describe under comments.

_____ Please check if you have visited one or more physical locations of the company on another occasion previously (recommended). Please describe under comments.

_____ Please comment on when the virtual site visit took place, duration and who was present and note if the virtual site visit took place over several occasions or a single session (mandatory)

Comments:

To be completed by the **Primary Sponsor**:

_____ I (sponsor) am familiar with the way the candidate team operates and attest that the applying team satisfies the minimum requirements for FIRST membership.

_____ I (sponsor) have met the applying team and presented FIRST and answered their questions.

_____ I (sponsor) have reviewed applicant's critical operational and managerial issues and acknowledge they are up to FIRST standards.

_____ I (sponsor) have had working interaction with the applying team.

_____ I (sponsor) have explained the confidentiality of the information that is passed within FIRST and the applicant agrees to comply with those policies outlined in the Operational Framework.

Any other comments/recommendations:

PRIMARY SPONSOR:	APPLYING TEAM:
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date: