

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	What
1.0	2006-Apr-13	Robin Ruefle (CERT Program) Damir Rajnovic (PSIRT)	First public release

FIRST Site Visit Documents Overview

As part of acquiring FIRST membership, a team must host a site visit from an appointed FIRST team. 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 <http://first.org/membership/>.

Additional documents have been created as part of the site visit process, The Best Practice Requirements document and the Site Visit Evaluation document.

The first document is a best practice guide for CSIRT-type organizations. This document discusses a best practice list of requirements which can be used in building or benchmarking a team¹.

The second document is a description of items to be reviewed by the site visit team during the FIRST membership application process. The items in this Site Visit Evaluation document are used to perform an assessment of the qualifications of the candidate team.

These documents are meant to introduce a more formal structure into the site visit process for becoming a member of FIRST. Although the documents are separate, they are intended to be used together. The Best Practices should be used in the early stage of team formation as a list of issues that the team may want to think about and address. Once into the team creation process, the team may want to use the site visit document as a checklist to verify if all important issues are indeed resolved. The same Site Visit Evaluation document will be again used by the sponsoring team to perform the site visit and the final validation before recommending a team for membership.

More information on the site visit and use of these documents is explained below.

What is a site visit and why is it done?

This is a frequently asked question. Potential FIRST members want to know what is accomplished during a brief visit and what its purpose is. The purpose of the site visit is to verify that the aspiring team satisfies the minimum requirements for FIRST membership. The main requirement is to protect the confidentiality of the information that is passed within FIRST. The second reason is to familiarize the site visit team with the way the candidate team operates. Lastly, this is an opportunity to meet candidate's team managers, present FIRST as an organization and answer any questions the candidate team might have.

Will site visit make the candidate trusted?

It will not. The site visit can not magically make a candidate team trusted by other members of FIRST or make the candidate team trust other FIRST member teams. The visit is only 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 interaction with other teams.

¹ This Best Practices document is envisaged but not developed.

Assumptions while conducting site visit

Both parties, 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 may, and will, ask for some documentary evidence related to the candidate. In order for the visit to flow smoothly it is suggested that the sponsor and the candidate team discuss this issue in advance. If possible the candidate should provide the requested documents. If the document exists, but can not be produced for any reason, the candidate should state so and provide as much detail orally as possible. The sponsor must note which documents were not available and the reasons why in the Site Visit Document checklist. An overview of the reviewed documents should be written in the final report unless the candidate objects to that.

How to do a site visit for a distributed teams?

If the candidate team is distributed over more than one physical locations, the sponsor must visit at least one site that is mutually agreed upon. It does not have to be the 'main' site if it exists at all. Any site will do fine. The assumption is that other sites are, at least, up to the same standard as one that is being visited. In the case that some of the other sites are not to the same standard as the visited site, the sponsor must note and enumerate all differences. In the opposite case, where other sites adhere to more stringent standards, the sponsor must just make the note of that fact.

What happens after the site visit?

After the site visit, the sponsor submits its findings to the FIRST Membership Committee, Steering Committee and finally to whole FIRST membership. At any stage additional questions can be raised and sponsor's duty is 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, can not satisfactory address it, the application will fail. As guidance, if less than 75% of mandatory items are not addressed satisfactory, the application has more chance of failing than passing. The FIRST Steering Committee has the discretion to intervene and accept candidates into membership irrespectively of the site visit results.

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.

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

No. The site visit is only a component of the process. The information collected during the visit will be given to the whole FIRST members for review. Only if there are no objections after the review the candidate by the FIRST membership, will the candidate be accepted.

Not all questions are relevant to a particular site visit

The site visit document is tailored to fit a profile of a generic team. Since the particular candidate may differ from that generic team some items may not be applicable to it. All these instances must be documented together with the reasons why they are not applicable.

In order to help candidates and sponsors, an appendix will be developed that provides different profiles which better describe some particular categories of candidates. One such category is a liaison member. The 'profile' consists of a list of items that should be relevant to a given candidate category.

How should the site visit report be submitted?

The report should be submitted in electronic form. After each item the sponsor must write the findings. If a checklist is included for a particular bullet then the appropriate box must be ticked by putting an 'x' in it. The sponsor should collect as much relevant information as possible. Any caveats and sponsor's deliberations, thoughts and comments must be noted too. Information should be collected in a single file and sent to FIRST Secretariat as a PDF document. The notes and information can be either typed in a document or written on a paper and then scanned. All submitted documents should be sent in a secured fashion.

Suggested Course of Action

Since candidates have a limited time frame to complete the application (currently six months) it may be a good practice to start verifying the candidate's status against this document before formally applying for the membership. If big discrepancies are found the candidate can take as much time as needed to resolve them without worrying about running out of time. If the review confirms that the candidate is in a good shape then the formal application can be submitted immediately and the whole process should be completed smoothly.

FIRST Site Visit Evaluation Document Introduction

As part of acquiring FIRST membership, a team must host a site visit from an appointed FIRST team. 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.

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**)

Understanding a CSIRT's constituency will help the team determine what needs they have, what assets need to be protected, and what the interactions with the CSIRT will be. Using this information will help determine what services need to be offered and what CSIRT organizational model will fit the needed service delivery.

Defining the constituency will also help scope the work of the CSIRT when it becomes operational. It will help determine what requests will be handled and what requests will be passed on to other CSIRTs or other relevant parties.

Each team must have a clearly defined constituency. If there is overlap with any other team that must be made known and the constituency must be clear when to engage which team.

This information should be advertised in any service brochures, incident reporting guidelines, or CSIRT descriptive information.

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 sector and type of constituency should be recorded.

Constituency type could be: internal, external or mixed.

Constituency 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 explain the purpose and function of the CSIRT in a clear, unambiguous manner. It should also list a brief overview of the core goals and objectives of the team.

The mission could be contained in a separate mission statement document or in a charter for the CSIRT or a similar document.

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

This is a formal document by which the CSIRT is established. This document not only establishes the team but outlines its approved operations and authority.

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 or the announcement from management mentioned in 1.3.

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 a similar document.

For a team to be successful, the constituency must know that it exists and understand how to engage and interact with the CSIRT. When a CSIRT becomes operational there should be an announcement to its constituency declaring it so and describing the interface with the constituency.

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**)

The CSIRT should have a defined set of services which 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.

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

The list of services defines what the CSIRT provides and what it does not provide for the constituency. It helps set the expectations for both CSIRT staff and constituency members about the roles and responsibilities the CSIRT will have.

Verification of such a list can be found in any brochures documenting the CSIRT's services and missions, or any similar types of documents, including charters, concept of operations, or handbooks.

To meet this requirement the list of services must not only be defined but also be advertised to the constituency.

1.5. A Funding model is in place (**Mandatory**)

To ensure long-term stability the CSIRT requires a funding model to be in place. This model will provide the CSIRT with incoming funds to ensure continued operation of the team and continued provision of CSIRT services to the constituency. If any charges are made to the constituency for services or subscriptions, they should be publicized to the constituency.

Funding for not only start up costs, but also for long-term operational, personnel, and facilities costs needs to be in place. A budget or financial plan or program should be in place.

The funding model can take many different forms; any are acceptable, as long as they are viable and provide the CSIRT with a stable source of funds:

The team can be a cost centre within an organization (the host or parent covers all expenses and does not receive any revenue from it). This is usually standard for an internal CSIRT.

The team can be funded in whole or in part by grants. If this is the case then the following questions should be asked. The answers will help the reviewer understand how stable the grants and the granting organization are which will help determine if this is a viable funding model.

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

the team could be funded through a consortium of organizations such as universities in a research network.

the funding model could be a combination of any of those listed above.

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 department, in the security group, in the IT or telecommunications department group, or even in the compliance division. The CSIRT could report to the CIO, the CEO, the CSO, another department head, or the CSIRT could have only its own manager.

A coordinating CSIRT for a broad constituency can be located within a centralized department or be its own organization. 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 basically details the CSIRT staff members, their roles and responsibilities, and their corresponding location in the parent organization or constituency. All team members may not be located in the same department, especially if they are remotely located or if they are a shared resource.

The team's organizational description can also include any sub-divisions or subgroups that the CSIRT may be divided into. For example, there may be a specific training team or a vulnerability handling team, etc.

This organizational description should identify any CSIRT Team lead and all core and extended staff.

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 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. 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 any categorizations or classifications of information that the CSIRT and its corresponding constituency have instituted.

This classification should make distinctions between sensitive, confidential, or public information.

The policy should cover at a high level how each classification of information should be handled for storage, transit, access, etc.

Any corresponding procedures should explain this at the detailed level.

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 different classifications of information are stored and protected. 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 can not be discussed on mobile devices such as PDAs, blackberries, and

phones; along with what information must be transmitted and discussed and stored in a secure fashion.

The policy should include specific statements that sensitive and confidential information should not be shared or discussed with non-authorized persons. There should also be statements that state that sensitive information should not be discussed on non-secured communication devices.

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 information is stored and protected, including how backups are handled, transported, and archived.

This policy should apply to information in any form; electronic or hardcopy.

2.4. Record destruction (**Mandatory**)

This policy should detail how information (electronic or hardcopy) is destroyed, based on its classification. This should detail how media such as hard drives, portable storage devices, etc. are destroyed so that sensitive information is not leaked or accessible to unauthorized personnel. It should also discuss how hardcopies of information are shredded and by whom.

The policy should specify that any information that is considered sensitive, site-related, or confidential should be destroyed only by those with approved access. It should also specify that information must be destroyed in a manner that it can not be re-constituted. The policy should detail the method for destruction for both hardcopy and electronic information formats.

2.5. Information dissemination (**Mandatory**)

This policy has a dual purpose: it should discuss the type of information that can be disseminated to various internal and external groups and it also should outline the methods by which information should be disseminated.

At the highest level, information dissemination policies outline what information can be disclosed to internal and external groups and organizations. They detail the specific types of information that should not be released and target what information should be considered sensitive or confidential.

This policy is extremely important to a CSIRT, as most teams survive based on their trustworthiness. 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 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 (in some cases, even legal requirements for external audits). For example, if another CSIRT reports an incident, what can its constituents expect regarding the disclosure of the information reported? Will it be reported to law enforcement or the CSIRT management? The policy should specify limitations, which should be made publicly available (to the constituents and other interested parties). Under what circumstances must a team pass sensitive (even contact) information to law enforcement or a court?

This policy should also outline the methods by which information is disseminated to various parties, whether through reports to management, advisories or alerts to the constituency, best practices available on a web site for the constituency, or other methods. This should include the defined documents types that a CSIRT might produce including the distribution mechanism and its frequency. Types of documents could include advisories, alerts, FYIs, technical procedures, and guidelines. The storage location for this information should also be detailed. Along with who maintains this information, who can access it, and who can provide information for it.

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.

A list that is kept up to date of authorized personnel who can see the different types of information is recommended.

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

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

All equipment used by a team must be secured against unauthorized access. Computers must not be left unattended with logged on sessions or confidential data left on the screen. If applicable, periodic checks should be conducted in order to determine unauthorized HW (e.g., keyloggers) and SW (e.g., keyloggers, trojans, and viruses).

This policy and corresponding procedures should outline

the appropriate use of systems

- Can systems be used for personal activities?

- What sites can and can not 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 should 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. These criteria should be based on how a computer security incident is defined within the CSIRT's constituency. Using this definition, different categories of incidents should be identified. Also methods and criteria for correlating and combining incidents should be established.

Issues to be defined include:

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**)

Incident reporting is just the first step in handling an incident. The central reporting point is not necessarily the same group who will research, analyze, and respond to an incident. 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

any special notification or interdepartmental communications that are necessary

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. This policy should support the information dissemination policy that outlines what information can be shared with these other teams.

The policy should define how the CSIRT interacts and cooperates with other CSIRTs. It should define not only any specific teams that the CSIRT has a formal interface with, but also the rules of engagement for working with those teams. This should include defined POCs, protocols for cooperation, and any special format for data-sharing.

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 infrastructure in place.

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 other provided services

- databases, data repositories, and data analysis tools for storing CSIRT and incident information
- mechanisms or applications for secure email and voice communications

Premises from where a team operates must satisfy some minimal security conditions in order that information could be adequately protected. Team's personnel should have some degree of privacy in order that non-team employees, or company's guests, can not easily learn information they are not entitled to.

If the team is dispersed then all locations should provide the same, or equivalent, level of privacy and protection. Variations are expected depending on the local circumstances. Example: office that does not accommodate visitors can omit some of the requirements related to handling visitors.

Apart from having premises team must poses some required devices and environment in order to conduct its business. Some of the devices that are required are computers, network (local and Internet access), telephones, shredders and fax machines. The list is not exhaustive.

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**)

Physical security encompasses, among other things, the following items:

- policy on accommodating visitors
- eavesdropping team's conversation (telephone or otherwise)
- access to teams premises and equipment (physical or otherwise)
- access to team's document archive (paper and electronic).

The list is not exhaustive.

Here is an alternative to this section:

Physical Security

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.

Thought should be given to locating CSIRT staff in offices with doors rather than cubicles. This will reduce the chance of sensitive information being overheard or seen.

Physical security requirements include

- 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, including some sort of access card

3.2. Equipment

Computers (**Mandatory**)

A team must possess computers in order to perform their daily operational tasks.

Telephones (**Mandatory**)

In order to be able to reach others, and be reachable itself, a team must have telephones. It is expected that telephones do have, at least, access to a public PSTN. They can also have access to any other private network as required. Telephones can be mobile, fixed line, radio-telephones, satellite phones, IP phones, soft-phones or any others. In all cases team members must be aware of technology limitations and what kind of conversations can be held using a particular device. If appropriate, they must advise the other party in the conversation on what kind of information can be shared during the call.

Fax

Fax is an optional device. If it is a dedicated fax device for exclusive team's usage then it can be used for sending and receiving all material. If it is shared among multiple groups then all reasonable effort must be used to inform senders of that fact and advise on what kind of information can be sent.

Shredders or other destructive mechanisms (**Mandatory**)

Paper shredders are the minimum that is required to exist. It can be either in a form of a shredder physically within the premises or as an outsourced

service. Shredder can be shared among multiple groups (that can have additional advantage since classified material is 'diluted' by other documents). The shredder must be cross cut shredder.

In the case of an outsourced service, the team must understand the arrangements and should have access to service audits in order to assess potential exposure.

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**)

Incident, and all other events, should be tracked. They can be stored in a sophisticated database, a paper log file, or simply as files in a file system. The actual mechanics are not as important as the fact that some system exists. If a large amount of incidents are expected to be received, then the system must be scalable. Additional requirements on the tracking system include having safeguards from unauthorized usage. It also must have audit capabilities so that it is possible to determine, at least, 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.

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.

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. The idea is to minimize risk of sniffing team's traffic.

Network separation can be either physical (the preferred option) or logical. Physical separation should involve a separation device (e.g., a router or firewall) between a team's network and the rest of the company. Ideally, the team should have its own Internet access too. Logical separation (e.g., VLAN) should be compensated by increased vigilance in monitoring significant events on the team's network.

Test network (**Mandatory**)

A test network is mandatory for testing unknown software. 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 separated from any other existing network. It may have its own access to the Internet. Logical separation (e.g., VLAN) can be acceptable as long as the team is aware of technological limitations and compensate that with additional vigilance on a production network(s).

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. This should cover items like: DNS, mail infrastructure, FTP and Web server, computers, data backup and handling backup media. The list is not exhaustive. The purpose is to identify possible weak spots where unauthorized information leakage can occur.

If the risk is considered higher than acceptable the team must devise and apply appropriate countermeasures to lower the exposure.

As part of the site visit, the site team may want to talk to the infrastructure provider to ensure all security requirements are being met.

Usage of Secure Communications (**Mandatory**)

The team may have requirements for using for secure communications or storing and archiving files in a secure manner. The site visit team should review what type of secure communications is used within the team. PGP is addressed in a separate item below.

3.6. Use of PGP (**Mandatory**)

Since PGP or GPG is required for communications in the FIRST community, how PGP is used in the team environment should be reviewed by the site visit team.

To be a member in FIRST, a CSIRT must maintain and use PGP encryption. Encryption keys must be distributed to all parties that will use it. Distribution method can range from public key repository (i.e., PGP keyserver), posted on the web site or sent on a CD or smart card. The exact method is less relevant as long as the constituency, and other potential users, know what it is and how to use it.

Questions to be asked include

Does the CSIRT have a team key?

Does the CSIRT staff have individual keys?

How are encryption keys distributed to the constituency and other collaborators?

This information can be verified by reviewing any team brochures or advertisement, web sites, or other communications mechanisms that discuss the encryption keys. The site team may also test that the encryption keys work, if this has not already been done.

Questions to ask may include

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

In this section of the requirements, the FIRST Site Visit Team will take a look at the methods, processes, and technologies used by the CSIRT to handle incidents. The purpose of this section is 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. The most common ways are: e-mail, telephone and fax. There are no prescribed communication channels so any one of those can be used. The main issue is that the channel is appropriate for the team (given the operational environment of the team and constituency) and that the constituency knows what it is and how to use it. 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 activity
- 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
 - 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 Handling Process (**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 criteria is 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. It is recommended that some type of acknowledgement be given for each incident report received. Acknowledgement can be done by a person or through an automatic mechanism.

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 (**Mandatory**)

Constituents need to understand how to contact and interact with the CSIRTs. To this end, a team's contact information should be advertised

internally and externally, as appropriate. It should be the same but that is not mandatory. In some cases a team may not want to advertise externally.

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?
- FTP?
- Email?
- Telephone or Hotline?
- FAX?
- RSS channels?

6. Professional development

6.1. Training (**Mandatory**)

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

Having a training plan is not sufficient. People must be given time to train and learn.

Questions to ask

Is there a prescribed training program or does each team member have to acquire training on their own?

How is training tracked and regulated?

Do job descriptions list required skills and abilities?

Is there a professional development program?

Are staff given time and resources to attend conferences and training?

6.2. Conferences

Attending conferences is vital to acquire new knowledge and to make connections with other teams and individuals.

Teams are encouraged to have members attend conferences.

To be considered an active team, someone from the team must attend at least one CSIRT-related event or conference. (**Mandatory**)

Questions to ask

Are there conferences that are attended regularly? What is the reason for selecting these conferences?

How many team members go to them? Are they always the same or they are rotated?