# **[Candidate] Site Visit Report**

## **[Date of Visit]**

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

INDEX

[General items 3](#_jgufiy7ta1o)

[Defined Constituency 3](#_ai1so74yhym)

[Mission statement or charter 3](#_cvqh6ov4cj4l)

[Document of creation, effective start date and announce 3](#_t9t3orscw4xu)

[Defined and advertised set of services provided for the constituency? 3](#_rszgsgpyje35)

[Funding models in place 4](#_wjzvr869h01m)

[Organizational Home 4](#_xo4tmt7pgw1b)

[Policies 4](#_jqgnp6zd9l0y)

[Information classification 4](#_4a4brx4w0rbk)

[Information protection 4](#_o5mk8tb4xxe4)

[Record Retention 4](#_g5e1t6nztn6n)

[Record destruction 4](#_ptwvg6seq0f6)

[Information dissemination 5](#_hcvmy69ozq7f)

[Access to information 5](#_lbew2s1jksmw)

[Appropriate usage of systems 5](#_b10rz8xboocp)

[Computer security events and incidents definition 5](#_s08j0llqx046)

[Incident handling policy 5](#_sausm14vis9d)

[Cooperation with other teams 5](#_5eg3ro89cw14)

[Any other policies 5](#_7zkuh7igp55f)

[Workplace and environment 5](#_cv37uvutr6js)

[Physical security and facilities 5](#_og9ic55zw1ir)

[Equipment 6](#_s7z7jr2iqaqr)

[Storage 6](#_l9kanl8mfcdl)

[Incident creation/tracking 6](#_a551kucaaul3)

[Network infrastructure 6](#_jntorn81nhch)

[Incident Handling 6](#_9wml6aqw4puw)

[How to report an incident 6](#_gggafbe2ir5i)

[Incidents can be reported by email 7](#_hl7095ynbken)

[Incident handling process 7](#_6t3lb31glsv5)

[Acknowledging report (optional, but recommended) 7](#_y4mtjv5ka8jg)

[Contact information and information dissemination 7](#_9lx3g4j0nmnp)

[Internal vs external 7](#_q3y9eyjrqv2c)

[Professional development 7](#_usseepiosvj6)

[Training 7](#_ulamzy9nl7a1)

[Conferences/Special Interest Groups 8](#_lkz1je4fge7k)

[Remote Visit (if applicable) 8](#_69kbgd7nvy1b)

[Signatures 8](#_af784cesblu6)

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*](https://www.first.org/standards/frameworks/)*.*

#### 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,* ***[Candidate]*** *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  Team Name  Date |  | Applying Team Representative  Team Name  Date |
| --- | --- | --- |