RFC-2350

Version 2.0 - 5 May 2023

Table of Contents

1 Document information

This document contains a description of TibCERT in accordance with RFC 2350. It provides basic information about TibCERT, its channels of communication, and its roles and responsibilities.

1.1 Date of the last update

Version 2.0 – March 5, 2023.

1.2 Distribution list for notifications

Currently, notification distribution is done through WhatsApp's public communities.

1.3 Locations where this document may be found

The current version of this document can be found at:
https://www.tibcert.org/assets/RFC2350.pdf

1.4 Authenticating this document

This document has been digitally signed by Lobsang Gyatso Sither, Director of Technology at the Tibet Action Institute.

Document Identification

Title	RFC2350
Version	2.0
Document date	5 May 2023
Expiration	Expiration This document is valid until superseded by a later version

2 Contact information

2.1 Name of the team

Full Name	Tibetan Computer Emergency Readiness Team
Short Name	TibCERT

2.2 Address

Near Dalai Lama Temple Gate, Mcleod Ganj, Dharamshala, Distt Kangra - 176219, H.P.(India)

2.3 Time zone

IST (GMT+5:30)

2.4 Telephone number

+91 1892292177

2.5 Electronic email address

For incident reporting, contact us at: submit@tibcert.org
For notification and support, contact us at: support@tibcert.org

These email addresses are monitored by a concerned staff member during office hours.
For non-operational matters, such as administration-related topics and general inquiries, please send us an email at: info@tibcert.org

In case of an emergency, please contact us by phone at +91 98824 07365

Our office hours are from 09:00 to 17:00 GMT+5:30 from Monday-Friday. We may operate outside of these hours and days only in an emergency.

2.6 Other telecommunication

Signal +91 8218207324

2.7 Public keys and encryption information

We use PGP for functional exchanges (notifications, incident reporting, etc.) with our peers, partners, and TibCERT members.

Fingerprint (info@tibcert.org)	58D6 8BCB FF96 67B6 56A3 5476 32B3 E86A D9C6 A868
Fingerprint (support@tibcert.org)	38A5 1596 F054 30BA AD11 1B6A 2D95 C52A 2072 13A4
Fingerprint(submit@tibcert.org)	CA53 1690 E79A AB62 298B BA75 868D 72F7 E1DC ADEF
PGP Key	Location of the key
Location	https://goo.gl/maps/L7513gDz3keWwcDe9

2.8 Team members

The TibCERT Director is Lobsang Gyatso Sither. TibCERT Secretary is Tenzin Thayai. The TibCERT Response Manager is Dorjee Phuntsok. TibCERT's sysadmin is Gemphel Norsang. The team includes around 10 staff members.

2.9 Other information

TibCERT is a member of:

- **CiviCERT,** which is an initiative of RaReNet (Rapid Response Network), an umbrella organization formed by the partnership between Internet content and service providers, Non-Governmental organizations, and individuals that contribute some of their time and resources to the community in order to globally improve the security awareness of civil society.

3 Charter

3.1 Mission statement

Our goal is to strengthen the Tibetan community's resilience for digital security by encouraging sustained collaboration among stakeholders, raising public awareness of online threats, and providing useful tools for defending against them. Our goal is to create a platform that promotes knowledge exchange and enables the Tibetan community to evade censorship and monitoring in Tibet through close collaborations with international cybersecurity specialists and frequent information and advice dissemination.

We operate according to the following key values:

- We uphold the highest ethical standards of integrity.
- We are highly service-oriented and operationally prepared.
- We promptly respond to cybersecurity incidents and emergencies with a strong commitment to resolving them.
- We aim to enhance and complement the existing capabilities of our members.
- We facilitate the sharing of best practices among our members.
- We cultivate an open culture within a secure environment that operates on a need-to-know basis.

3.2 Constituency

The constituency of TibCERT is composed of Tibetan diaspora stakeholders, including CSOs, institutions, monasteries, media groups, Tibetan communities, and Tibet Support Groups worldwide.

All organizations serving the Tibetan community are eligible to contact TibCERT and request assistance.

3.3 Sponsorship and/or affiliation

TibCERT is a Tibetan community driven initiative supported through grants and donations from members.

3.4 Authority

The scope of TibCERT's authority is limited to coordinating security issues on behalf of its stakeholders. Nevertheless, TibCERT is intended to provide operational guidance on vulnerabilities, incident mitigation, and/or incident response. Blocking addresses or networks is one suggestion among many that might be made. TibCERT is not responsible for ensuring that these suggestions are followed; instead, it is the stakeholders to whom they are directed.

4 Policies

4.1 Types of incidents and level of support

TibCERT is authorized to address all types of computer security incidents that occur, or threaten to occur, in our stakeholders and that require cross-organizational coordination.
The level of support given by TibCERT will vary depending on the type and severity of the incident or issue, the type of stakeholder, the size of the user community affected, and TibCERT's resources at the time. Special attention will be given to incidents involving personally identifiable information.
Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. TibCERT will support the latter people.
TibCERT also acts as a coordination center. Members of the public who identify vulnerabilities in a web site or software that affect the Tibetan community are welcome to report them to TibCERT. TibCERT will coordinate the resolution of the vulnerability with the affected group.

4.2 Co-operation, interaction, and disclosure of information

All incoming information related to incidents is handled confidentially by TibCERT, regardless of its priority.

We take the security of sensitive information seriously and have implemented measures to ensure its confidentiality. When reporting an incident that involves sensitive information, please label it as "SENSITIVE" and use encryption if possible. Our team follows the information sharing Traffic Light Protocol, meaning that we handle information with the tags WHITE, GREEN, AMBER, or RED (https://tibcert.org/#tlp) appropriately. We only share information with relevant parties on a need-to-know basis and preferably in an anonymous manner. If you have any concerns about our usage policy, please inform us, and TibCERT will try to follow your guidelines while ensuring that we can take appropriate action to resolve the issue.

4.3 Communication and authentication

For non-sensitive communications, TibCERT uses conventional methods like unencrypted email.
For secure communication, PGP-encrypted email is preferred (see Section 2.7). If it is necessary to authenticate a person before communicating, this can be done through existing networks of trust in the community. X.509 signed e-mail messages will be authenticated, but will be responded to with PGP signed email. TibCERT communicates in English; however, incidents may also be reported in Tibetan.

5 Services

TibCERT assists all its stakeholders in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the pre-incident, regarding an incident and post-incident
5.1. Pre-incident :- Security Audit, digital security policy implementation, digital security training

5.2. Incident handling:-

5.2.1. Incident Triage

1. Determining whether an incident is authentic;
2. Assessment and prioritizing the incident.

5.2.2. Incident Coordination

1. Containment: containing the incident and determining the scope of the incident, implementing appropriate measures to contain the incident.
2. Eradication: Eradicating the artifact from victims system
3. Recovery: Putting back the system in the regular work force.
4. Sending acknowledgements and alerts regarding the incident.

5.3 Post-incident:- Lesson learnt session and best practices

6 Incident reporting

Currently, there are no local forms available, and no particular reporting format is required to report an incident to TibCERT.

Reporting can be done through unencrypted email at submit@tibcert.org or preferably encrypted with our PGP public key,

However, we also accept incidents through our Twitter handle and Telegram messages. When you contact us, please provide at least the following information, if possible:

1. Provide contact details and organizational information, including the name of the person reporting the incident, the name and address of the organization, email address, and telephone number.
2. Provide a brief summary of the incident, emergency, or crisis and the type of event that occurred.
3. Indicate the source of the event or incident, such as the system that produced an alert.
4. Identify the affected system(s) that were impacted by the incident.
5. Estimate the impact of the incident, such as any loss of communications or other disruptions.
6. Include any additional information that may be relevant to the incident, such as details of the observations that led to its discovery, scanning results (if any), and an extract from the log showing the problem. If forwarding any suspicious emails, please ensure that all email headers, body, and attachments are included. TibCERT follows the CERT-XLM Security Incident Classification standard.

7 Disclaimer

While all precautions have been taken while preparing this document, information, notifications, alerts, and responses to security incidents, TibCERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained in our guidance.