National CSIRT of Mongolia
RFC 2350

1. Document information

This document contains a description of National CSIRT of Mongolia in accordance with RFC 2350[1] specification. It provides basic information about National CSIRT of Mongolia, describes its responsibilities and services offered.

1.1 Date of last update

Version 1.1, published on January 27, 2025.

1.2 Distribution list for notifications

Changes to this document are notified to:

- APCERT – https://www.apcert.org/
- FIRST – https://www.first.org/
- TF-CSIRT– https://www.trusted-introducer.org/
- Technical PoC for the OSCE Cyber/ICT security CBMs https://www.osce.org/secretariat/cyber-ict-security

1.3 Locations where this document may be found

The current and latest version of this document is available at National CSIRT's website at:
https://ncsirt.gov.mn/p/15
Please make sure you are using the latest version.

1.4 Authenticating this document

This document has been signed with the PGP key of National CSIRT of Mongolia.
The signature and our public PGP key (ID and fingerprint) are available on our website: https://ncsirt.gov.mn/p/30

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Contact information

2.1 Name of the team

Official name: National CSIRT of Mongolia

Short name: NCSIRT

2.2. Address

Mongolia, Ulaanbaatar 15160, Chingeltei District, Juulchin Street-3

2.3. Time zone

UTC+08:00 (Ulaanbaatar Time)

2.4. Telephone number

Main number: +976 1800-1118

2.5. Facsimile number

Not applicable

2.6. Other telecommunication

Not applicable

2.7. Electronic mail address

For reporting incidents, cyber threats, or other operational matters, please contact incident@ncsirt.gov.mn. This address is monitored by a duty officer during and outside regular office hours.

For non-operational matters, including administrative issues, cooperation, or general inquiries, please contact contact@ncsirt.gov.mn. This address is monitores by the National CSIRT's Communications Unit druing office hours.

2.8. Public keys and encryption information

National CSIRT uses PGP for secure communication.

- Key ID: 88D74F1060E87C4E
- Fingerprint: 824E F5A4 45DA 377A 4876 4334 88D7 4F10 60E8 7C4E

The public PGP key is attached to this document.

2.9. Team members

The National CSIRT is composed of 4 specialized units, each dedicated to specific areas of expertise.

- Security Operations Center
- Incident Response Unit

- Cyber Threat Intelligence Unit
- International Cooperation and Communications Unit.

Information regarding the composition of these units and their personnel is not publicly disclosed. Identities may be shared on a case-by-case basis, in accordance with the need-to-know principle.

2.10. Other information

See our web site at https://ncsirt.gov.mn/ for additional information.

2.11. Points of customer contact

The preferred method of contacting National CSIRT is via email (as per § 2.7). National CSIRT encourages its counterparts to use secure email when sharing sensitive information. Alternatively, National CSIRT may be contacted by telephone (as per § 2.4).

National CSIRT's regular working hours are Monday to Friday, from 08:30 to 17:30 (local time). However, a duty officer is stationed until midnight to ensure continuous operational coverage.

3. Charter

3.1. Mission statement

Safeguarding Mongolia's digital landscape through unified defense leadership, rapid incident resilience, and fostering international cybersecurity collaboration.

Unified Defense Leadership: Coordinate and lead a cohesive national response against cyber threats, ensuring synergy and effectiveness in safeguarding Mongolia's digital landscape.
Rapid Incident Resilience: Swiftly detect, terminate, and respond to cyber-attacks on state-owned legal persons with critical information infrastructure and organizations connected to the state information consolidated networks, prioritizing speedy recovery and resilience of essential systems.
International Cybersecurity Collaboration: Represent Mongolia globally, collaborate internationally, and set proactive cybersecurity standards, contributing to a secure digital environment for national and global well-being.

3.2. Constituency

In accordance with Article 21.2.2 of the Law of Mongolia on Cyber Security, the constituents of the National CSIRT are located across the territory of Mongolia and include state-owned legal entities operating critical information infrastructure, as well as organizations connected to the State Information Consolidated Network.

Pursuant to Article 21.2.1, the National CSIRT is entrusted with coordinating and facilitating the activities and operations of centers responding to cyber-attacks and incidents nationwide, and with providing professional and methodological support to these entities.

On the basis of this mandate, a range of secondary constituents, including private sector partners, academic and research institutions, cybersecurity professionals, and the wider public also benefit from a limited set of services delivered through the National CSIRT's information sharing, analytical, and coordination functions, notwithstanding the fact that they do not formally fall under its authority.

For more information, please refer to the Law of Mongolia on Cyber Security available on our website under the "About Us – Legal Act" section.

3.3. Affiliation

National CSIRT is part of the Information Security Department in the General Intelligence Agency of Mongolia.

3.4. Authority

Pursuant to the Law of Mongolia on Cyber Security, adopted on 17 December 2021, the National CSIRT was formally established under the structure of the intelligence agency. Article 21.2 of this Law defines the mandates and core functions of the National CSIRT including nationwide coordination and facilitation of incident response, detection and mitigation of cyber-attacks, provision of professional and methodological assistance, information analysis and dissemination, and representation of Mongolia in international cybersecurity cooperation.

In addition, the Government of Mongolia, through Decree No. 318 of 30 August 2023, approved the National CSIRT Rules and Working Policies to Combat Cyber-Attacks and Cybersecurity Incidents. This decree provides the institutional and operational framework for the National CSIRT's activities, further clarifying its role, responsibilities, and coordination mechanisms within the national cybersecurity architecture.

4. Policies

4.1. Types of incidents and level of support

The National CSIRT serves as the central point of contact for security-related computer incidents in Mongolia. It is authorized to address all types of cybersecurity incidents that occur or pose a threat to its constituents, in accordance with its national mandate.

The level of support provided will vary depending on the type and severity of the incident, the nature of the affected constituent, the significance of the impact on critical or essential infrastructure and services, and the resources available at the time of the incident.

The National CSIRT delivers both reactive and proactive services, focusing its efforts on incidents that have the greatest potential impact on national security, critical information infrastructure, and the continuity of essential services. Lower-priority incidents are addressed as resources permit, ensuring that all reported cases receive a timely and appropriate response.

4.2. Co-operation, interaction and disclosure of information

The National CSIRT operates in full compliance with the Law of Mongolia on Cyber Security and adheres to applicable legal, regulatory, and ethical requirements governing the protection and disclosure of information. Incident-related information, including names,

technical details, and other sensitive data, is not published without the prior agreement of the involved stakeholders. Unless explicitly agreed otherwise, all information provided to the National CSIRT is treated as confidential. The National CSIRT does not disclose information to third parties, except where required by law or where such disclosure is necessary to respond effectively to an incident in cooperation with trusted partners.

Within the National CSIRT, information is shared strictly according to its classification and the need-to-know principle. Only relevant and, where appropriate, anonymized extracts are distributed internally or externally. When information is provided under the Traffic Light Protocol (TLP), the National CSIRT fully complies with the information sharing policy defined by FIRST (see https://www.first.org/tlp/).

The National CSIRT is actively engaged in national, regional, and international cooperation frameworks (see § 1.2) and strongly supports voluntary collaboration between CSIRTs at all levels. To this end, the National CSIRT ensures a global presence and strong networking with its partners through active participation in working groups, international meetings, and conferences.

Information sharing with government bodies, law enforcement agencies, sectoral CSIRTs, critical infrastructure operators, vendors, and trusted international partners is carried out responsibly and securely, supporting effective incident response, vulnerability mitigation, and situational awareness, while respecting confidentiality and legal obligations. Interactions with the media and the public are managed in coordination with the relevant government communication channels. The National CSIRT does not disclose operational or sensitive information to the public unless authorized or legally required.

4.3. Communication and authentication

The preferred method of contacting National CSIRT is via email (as per § 2.7). For the exchange of sensitive information and authenticated communication National CSIRT uses PGP for encrypting and/or signing messages. All sensitive communication to National CSIRT should be encrypted with our public PGP key as detailed in Section 2.8.

5. Services

5.1. Incident response

National CSIRT's incident response services are continuously available to our constituency. All information and communication technologies related incidents are evaluated. In depth analysis is provided by technical experts.

5.1.1 Incident triage

- Assessment and verification of the severity of the incident (SOC);
- If required, escalation to the duty officer (IRT);
- If required, escalation to the Director of the National CSIRT.

5.1.2 Incident coordination

- Categorization of the incident-related information (log files, contact information, etc.) with respect to the information disclosure policy;
- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.1.3 Incident resolution

- Analysis of compromised systems;
- Assisting in remediation, including closing vulnerabilities and mitigating damage.
- Supporting system recovery and ensuring restoration of normal operations.
- Conducting post-incident reviews and recommending security improvements.

5.2. Proactive activities

Beyond incident response, the National CSIRT carries out a range of proactive services to enhance the cybersecurity posture of its constituents and the wider community. These include:

- Disseminating alerts, advisories, cyber news and best practices at https://ncsirt.gov.mn/;
- Providing security recommendations and technical guidance through trusted channels and its official website.
- Monitoring cybersecurity trends and threats at national and international levels.
- Sharing relevant intelligence with constituents to support early detection and prevention.
- Organizing seminars, workshops, and exercises to improve technical and operational readiness.
- Assist in performing vulnerability assessments in information systems upon a constituent member's request.
- Collecting and analysing incident data to identify trends, produce reports, and inform policy decisions.

6. Incident reporting forms

An incident can be reported via the official email (as per § 2.7), by telephone (as per § 2.4), or through the incident reporting form available on our website: https://ncsirt.gov.mn/cyberIncident/feedback

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, National CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

PUBLIC KEY NATIONAL CSIRT OF MONGOLIA
EMAIL ADDRESS: INCIDENT@NCSIRT.GOV.MN
PGP FINGERPRINT: 824E F5A4 45DA 377A 4876 4334 88D7 4F10 60E8 7C4E

-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBGWyKeABEAC7KnQLZ6e5X+sPmse/Zt1jgXenhQZaND3D2ACIjKt+YmD1
dzOW75fQSC1oKyZLQghYKSPhT3S6mijhStOc2or5yLppEGoacYX8Nt6ZE68m
rZo7MELE3H53nWcHWxXZ1XLRyad49eID0t8T6otrg5TKx4kaMRmTSEixf05D
vZZZxmeUikH3m3e6ED7HWHzlB5qdpLJLf7Ttzk36Qwk8S5hS6Yc36QxLKJ+H
VLhbppeyhRP709enVHd0xKp/3HqPnu+GQql4+ClkF/CJ1QiWvm0/abypqGkV
IQ/Rsbem3U+FSJ/WR5ygmGN+i6YPG8q4tN+pMxkgrIdrKoqjXiPN9CqrS23R
oIwB1LBfBYZARVR99J9EMwXPuiegH5+opIfsjuatXFWbfzv2Hw2RLrU0HJMi
UuJ8YUCOj6V9L0EsU7iiVVVhiYpz12RttGe2lWjue/TAoFCNciLqyS1mATze
MHlPtVtzp6IkA5SttO/LWyVDt8414vvmwziqq6sNYMMA4VcQTfywQAIFK6sY
HZYnE2ooDMBTY3U/44JXguZkNkkTX3js6JkUo1EgajGv6UZlnKqLrrWEJ9jT
wt6dvK7iuqro3e8ZhIHqgShFAmfLouHtpgqacouzvOE+vVNuqqNNS1VnuBhy
uEFSrfz8BVACi+iCx5o6re2G9Ao7Wbysx9BwLwARAQABzStJbmNpZGVudCBv
ZiBOQ1NJUlQgPGluY2lkZW50QG5jc2lydC5nb3YubW4+wsGKBBABCAA+BYJl
singBAsJBwgJkIjXTxBg6HxOAxUICgQWAAIBAhkBApsDAh4BFiEEgk71pEXa
N3pIdkM0iNdPEGDofE4AAFI7D/9lO105MDiEMzyKs8770cXzbA2JpLeOOhu+
BIpSGk/1YvaP4v9kL0yuTYBbUF5t3qPBjclpDQYBgy/RYh6reEhsG0xyJlDa
3dOz2Eoihm31zPQg/6zo+35rXk5WOx4jKFTxQnuTGq2Psw7DRkNqMJwypc9S
ZfDRzpc4zd0/7R642w6zdZFFBt5Uh1Lhme0CSxkC6ooOhCt3DqDC3Un+YDK0
e1jJzVpHtvZ7K8RkF/B11YH+KnfvhGIrURDpHH+Tzv+MAmYiVhFusJL1DN5N
GVGhiirFRoak3UBBnAdv4/8MUfSCOd3At3YtZp+fYwD+3U4OKSCsWYjzQdu3
R/p3I2rDwizGqhpjRnIaTP6vFLxxZpkC7vVvogAg7AC6Lv2c1Y72rL1XMhi9
+5JdXNICXnZvmt6CeT/OV+yDe8UwRQdhevL+uqDAE38Jr3lVOtcSbcgtJgIS
BUIeMCtjcXvdLTve0FDfJJRYbD+sHk0he3dacohrP/NJ4RBs10XwDPP2eq2r
G0Wk5UOAqVdgsmjlqxZzlXaDm5oSKE4E+UBDFyY4PCFtMFV1X3W2zKpl17B1
t6konSB1F7AW/KkJ9PAqVOf59KhgA6p0gLJ4Ji3tp36x1lMPGjeNk4BdjLoE
NZJRWG1N+FWxBLif5SqLwgg1NA04jVZY7CnSKCtRbmSzncZGz87BTQRlsing
ARAA3om3EgWaqiNj58AUG3DkHJxvoPSew+Z7Yj2x/gBiBbTNWUDvbUBSlvYl
BP3WCrGasTnQ4YDAabVkQpsBah9L26fwrByVJpZdn+ramSwT2EPqC600ewAT
oULDfoDtLtGZrSV+wPXrTHpV833pOvSyRO9ICSeeSsdPPa3wa0hGxQe1c2iA
AGazoRDXNgiV4YzDbEEEyJW+zLHrO3oHvoMjHlsOlMYEm860NmdYajQ1hmPd
IRdS+7giHYN6wEvb28Q1LYy+BphqHY4nPXj4grH4uZNdQY4YW9oBoLyo4LGd
RqDlN2M9BvtLhLt9yOtbqFBIA12kG3jURAXOg6lVAl7f7xRZWMfbrcBdxNA4
ihowY6N58Gdo5xNa4z05q+n+Av4vfcI2Bjddfwk0HS+xPEoLO+J0/9XrGv80
gUPr4/DceDKRQqJY4nQvXwLmpQuoWjnJr8CrARW1je9IGBWK5u71su/xdeId
MyECeFE0bxoIsGBlRrRe877fm+Q/Wy1KK8bglN3fVTPkGL3xMMWoYkQ8q8H/
zk/t7lSpCO+s5hQK67HfYEltPkMzi4bi2+ykk5/+QxkusCL9gfz1Tc50cRVB
yoMuYRU0trFtZgmvOjyU4gm0DWGb3AMjLG81NuhO6mieH/kkoNU68Afrwcrb
D0msMX4Jj83rAoy4kOqn1GPf9LcAEQEAAcLBdgQYAQgAKgWCZbIp4AmQiNdP
EGDofE4CmwwWIQSCTvWkRdo3ekh2QzSI108QYOh8TgAAnBkP/2SmHUUxmjvz
9eNarZFnJnRFfaESF0yO0P8FwbEW4SMfJ70qY4VdYsY6+L69EjKM9Xqw7Kci
z0MUnx/Gczm31cJMqeCsV/OzzG2k4SDviZlWjDydeI+bwxsgofiohDbRP48U
h/SObRsE1T1qjm6grgrJfSYfRr+rKdz2yMU5+XuZpUBt0B9SKaIc0A0eera/
aqSZ2ugKcDp186XSBDdg6Vp+p7RC8pOM1Fn9vvUvlp+623OQbvAbNa+JKVn5
R0WCeS/PmOn2p0afpRdQkcszyYb9ucI9DAdu57rBdMe41h0h+PCNdR7Z7BEn
xpjwL5Yh2vaehL2eaE6mKH77SIpJYJ5Beoy4Fkitkr9U+8IBK9lLVxVKiJAh
hFqXHQsc4U+bbULI+/aXTepkHZR4P+0ltdA8t2dGmEQJOFtmZk3/xLtxd9NA
j9l9DhhJuK6a/a5x+icukUL0qVAMMpygTDAMhjWIYlb59RpM30+nulCJnVe9
TJsDp//04mBiywGVsH3+3tkIltWfs2Dj1tFHXAksdlIXA5Yq3xUm1gxwifO2
3H+WLWbFHybIxz2AV7uoka+mPGmOv0bE4uMqY4BN6Xk3euqJb3a3T1iy/2k6
QpEd0eWkBDJl8hovMJJblbX5TbKk3TKd3aMm7rEebgTIPBnDWnrqA/tvoh1I
8drXhaD+8Uo2=dJUa
-----END PGP PUBLIC KEY BLOCK-----