RFC 2350

CSIRT-FORENSICS

TLP: WHITE

A Coruña. Wednesday, February 4, 2026

Approved by SOC Manager and DFIR Service Responsible (IR Leader). Security Officer reviewed

Content

1. CHANGE LOG

VERSION	DATE	REVIEWER	SUMMARY OF CHANGES MADE
1.0	05/09/2024	FORENSIC & SECURITY	**First version**
2.0	04/’2/2026	FORENSIC & SECURITY	**Second Version**

Approved by SOC Manager and DFIR Service Responsible (IR Leader). Security Officer reviewed

2. DISSEMINATION

2.1. Recipients of the document

The recipients of this document are the clients of CSIRT-FORENSICS, as well as any other established CSIRT or organization with a legitimate interest in the services provided, and the general public. Consequently, the document may be freely distributed, being subject solely to copyright controls.

2.2. Introduction

This document contains all the information that CSIRT-FORENSICS considers relevant for the potential recipients of the document described in the previous section. The document is organized according to the model recommended by IETF RFC 2350, available at **https://tools.ietf.org/html/rfc2350**.

2.3. Date of last update

The date of the last update, together with the document version history and the changes introduced in each of them, are reflected in the **Change Log** section of this document.

2.4. Locations where this document can be accessed

The document is publicly accessible through the Forensic & Security website, specifically in the section corresponding to CSIRT-FORENSICS:

https://www.forensic-security.com/en/csirt/ .

2.5. Authentication of the document

This document has been signed with the PGP key of the soc (at) forensic-security [dot] com account of CSIRT-FORENSICS. Both the public key and the signature are available on the CSIRT-FORENSICS website:

https://www.forensic-security.com/en/csirt/.

2.6. Distribution list for notifications

There is no distribution list for notifying changes to this document. New versions, when generated, will replace the previous one at **https://www.forensic-security.com/en/csirt/**.

3. Contact information

3.1. Name of the CSIRT

CSIRT-FORENSICS.

3.2. mailing Address

C\ Copérnico 3

15008 A Coruña (A Coruña)

Spain

3.3. Time zone

Central Europe (CET/CEST).

3.4. telephone number

+34 881 28 99 18

3.5. Fax number

No fax number is available.

3.6. Email addresses

Incident reporting and management: **soc (at) forensic-security [dot] com**

Enquiries: **consultas.soc (at) forensic-security [dot] com**

3.7. Other telecomunication

No means of communication are available other than those indicated.

3.8. Public keys and encryption

CSIRT-FORENSICS uses the soc (at) forensic-security [dot] com address for communications related to incident response, with the following PGP key:

Fingerprint: 1469 C680 3E62 0514 53F2 EE8E 2A96 7415 A52E 6142

This key is available at the web address mentioned earlier in this document.

PGP encryption must be used in all email communications that, due to their level of confidentiality, require.

For administrative communications or enquiries, the consultas.soc (at) forensic-security [dot] com address is used, associated with the following PGP key:

Fingerprint: 4143 510E 4FFB 460B 16D1 2C33 A606 B888 6726 7431

3.9. Team members

The team is made up of staff performing the following roles:

- CSIRT Security Analyst (L1 level)
- CSIRT Security Analyst (L2 level)
- CSIRT Security Analyst (L3 level)
- CSIRT Security Trainer
- CSIRT Administrator
- CSIRT N1 Technical Manager
- CSIRT Technical Manager
- CSIRT Architect
- CSIRT Process Consultant
- Forensic & Security Group Legal Consultant
- Forensic & Security Group IT & Multicustomer Services Director
- Forensic & Security Group Executive Technical Director
- Forensic & Security Group Finance Director

For privacy reasons, the list of personnel belonging to the team is not published in this document.

3.10. Operating hours

CSIRT-FORENSICS operates 24x7.

3.11. Additional information

For additional information related to CSIRT-FORENSICS, please refer to the Forensic & Security website, and more specifically the CSIRT section:

- **https://www.forensic-security.com/en/csirt/**

3.12. Points of contact

The main contact channel with CSIRT-FORENSICS for the communication and management of security incidents is email, through the address:

- **soc (at) forensic-security [dot] com**

Telephone contact is also available as an alternative means, using the number indicated previously:

- +34 881 28 99 18

For other types of communications, the following address may be used:

- **consultas.soc (at) forensic-security [dot] com**

4. Objectives

4.1. Mission statement

Organizations operate in increasingly complex environments, subject to demanding requirements for flexibility and availability in relation to how users consume applications and services. In this context, the traditional perimeter is disappearing and the attack surface is expanding, requiring specific adaptation of security processes.

In addition to this new reality for organizations, the attacks and methods used are becoming ever more sophisticated and diverse, leading to a “professionalization” of attackers and leaving everyone increasingly exposed to cybercrime. Likewise, the devices and security solutions available are also becoming more sophisticated and diverse.

There are also a number of legal obligations which, depending on the sector, must be taken into consideration, ranging from the mere notification of incidents to the requirement to have a CSIRT.

In this context, CSIRT-FORENSICS is a private CSIRT created by mandate of the Management of the Forensic & Security Group, with the aim of providing both internal services (internal CSIRT) and external services to other bodies and companies, whether public or private (commercial CSIRT). The mission of CSIRT-FORENSICS is to respond to the aforementioned cybersecurity challenges by making available to the entire Forensic & Security Group and its external clients the security services needed to protect their information systems against security incidents that could affect the integrity, confidentiality or availability of information and/or damage the operations or reputation of those affected.

In this way, the benefits that CSIRT-FORENSICS aims to provide its clients are:

- Improving real-time visibility of their cybersecurity posture.
- Anticipating potential threats and reducing the attack surface.
- Detecting incidents at an early stage and containing them quickly.
- Responding effectively to security incidents and limiting their impact.
- Restoring operations in the shortest possible time.

In order to fulfil its mission, CSIRT-FORENSICS:

- Offers a set of services, described in **Section 6** of this document, which may be contracted individually or in bundles, according to the specific needs of each potential client.
- Has highly qualified and experienced information security personnel, capable of delivering the services offered, as well as analyzing and responding appropriately to any security incident.

- Has the necessary and appropriate set of procedures and tools for the provision of the services offered.
- Performs continuous monitoring, centralizing visibility of activity and potential threats from all the elements or tools of an organization through a SIEM, significantly reducing the time required to detect possible incidents, identifying which threats require immediate intervention and which are false positives.
- Carries out proactive and preventive activities to enhance the security of its clients.
- Exchanges technical information on incidents with other CSIRTs in order to improve the collective response to them.

In order to maintain the highest standards of quality and compliance in the performance of its mission, CSIRT-FORENSICS:

- Has the policies and procedures necessary to ensure compliance with the legal requirements applicable to the services provided.
- Periodically, it carries out security audit processes on the services provided, basing them on standards and regulations commonly recognized in the sector, such as the National Security Framework (Esquema Nacional de Seguridad).
- Applies best practices commonly recognized in the sector, taking as a reference for its establishment and operation the guidance set out in RFC2350 (Expectations for Computer Security Incident Response), available at **https://datatracker.ietf.org/doc/html/rfc2350**, and seeking membership in the FIRST (Forum of Incident Response and Security Teams) organization, **https://www.first.org/**.
- Establishes strict requirements for ethical conduct and confidentiality for all personnel belonging to the service.

4.2. Constituency

The services provided by CSIRT-FORENSICS are aimed at all departments of the companies belonging to the Forensic & Security Group, as well as external companies and/or organizations, whether public or private, that subscribe to those services.

4.3. Affiliation

CSIRT-FORENSICS is a service operated by Forensic & Security Group and reports to Senior Management. The service is led operationally by the SOC Manager and the DFIR Service Responsible (IR Leader)..

4.4. Authority

CSIRT-FORENSICS operates under the authority of Senior Management. For governance, compliance and alignment with ISO 27001 and ENS, CSIRT-FORENSICS coordinates with the Corporate Information Security Officer.

Approved by SOC Manager and DFIR Service Responsible (IR Leader). Security Officer reviewed

5. Policies

5.1. Types of incidents and level of support

CSIRT-FORENSICS provides detection, analysis and response services for security incidents that may affect the integrity, availability and/or confidentiality of information managed by the systems and processes of its clients.

The typology of security incidents handled correspond to those established by the Spanish National Cryptologic Centre, CCN-CERT, using as a reference the ICT Security Guide CCN-STIC 817 for Cyber Incident Management in the scope of the National Security Framework (ENS) (**https://www.ccn-cert.cni.es/en/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file?format=html**). Following these recommendations, security incidents are classified according to their type and criticality, with response times being established based on this classification.

The level of support provided in each case will depend on what has been contractually agreed with each CSIRT-FORENSICS client.

The level of interlocution during incident management, the channels to be used, the information that may or may not be exchanged with other stakeholders, such as other CSIRTs, and the level of protection to which the information must be subjected will be defined with each client at a contractual level, or, if necessary, at the time the incident is detected, always respecting the legal framework and the regulations governing such communications.

5.2. Co-operation, interaction and disclosure of information

In its daily operations, CSIRT-FORENSICS interacts with a significant number of stakeholders, with whom it exchanges various types of information depending on the role each plays in its relationship ecosystem.

These actors can be other CSIRTs, legal authorities, sources of information and intelligence, customer organizations, suppliers, manufacturers, press, and within each of them, communication can be established with personnel who play very different roles, such as security engineers and analysts, system administrators, legal experts, security managers, HR managers, end users, or journalists.

Among all these actors, there are 3 that, due to their special relevance in the Spanish national sphere, are identified in this document:

- CCN-CERT (**https://ccn-cert.cni.es/en/**), to which relevant information and systems security incidents affecting public bodies and companies are reported.
- INCIBE-CERT (**https://www.incibe.es/en/incibe-cert**), to which relevant information and systems security incidents affecting citizens, organizations and companies in the private sector are reported.
- ESPDEF-CERT (**https://emad.defensa.gob.es/en/unidades/mcce/index.html?__locale=en**), to which relevant security incidents that could affect the sphere of national defense are reported.

- Spanish Data Protection Agency, AEPD (**https://www.aepd.es/en**), in cases where the incident has endangered or caused the disclosure of personal data protected by the European General Data Protection Regulation (GDPR) and the Organic Law on Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), which regulates the processing of personal data in Spain.

Furthermore, establishing formal cooperation relationships with other CSIRTs is considered essential, and at the time of drafting this document the process of joining the FIRST (Forum of Incident Response and Security Teams) community, **https://www.first.org/**, is being initiated.

In this scenario, it is critical to establish a clear procedure specifying what information can be exchanged in each situation with each type of stakeholder.

CSIRT-FORENSICS, following the information security policies of the Forensic & Security Group, establishes the following information classification levels:

- **CONFIDENTIAL**: Information handled within the owning body or organization, which can only be accessed by a limited number of people.

- **RESTRICTED**: Information handled within the owning body or organization, which can be accessed by internal staff, subcontractors and interested third parties. Recipients may be generic groups of people, for example, belonging to a specific department.

- **INTERNAL**: Free internal distribution but requiring express authorization for external distribution.

- **PUBLIC**: Information for public use, whose distribution does not negatively affect the interests or operations of the owning body or organization.

To facilitate cooperation, distribution and information sharing with clients, bodies or other CSIRTs, an equivalence is established between this classification and the FIRST TLP protocol, which will be used by CSIRT-FORENSICS to label information and apply subsequent protection measures based on such labeling.

Information classification. Forensic & Security Group	FIRST TLP Protocol equivalence
CONFIDENTIAL	TLP:RED
RESTRICTED	TLP:AMBER
INTERNAL	TLP:GREEN
PUBLIC	TLP:WHITE

Information owners are responsible for classifying it and indicating how and with whom the information may be shared based on that classification. CSIRT-FORENSICS undertakes not to share information with other parties without a prior agreement and authorization from its owner, except in cases where a higher-level legal or regulatory obligation requires that information to be shared.

As additional measures, beyond the above, CSIRT-FORENSICS undertakes to:

- Apply at all times appropriate technical and legal measures to protect information.
- Anonymize, as far as possible, shared information and, within it, select exclusively data relevant to resolving incidents.
- Protect the privacy of personal information. Although, as a general rule, personal data will never be shared, if it is necessary to do so, and within the circumstances permitted by European and Spanish regulations on personal data protection, the explicit authorization of the data subject will be requested.
- Stop the distribution of information at the moment its owner notifies the withdrawal of permission to do so, except in cases where a higher-level legal or regulatory obligation requires that information to be shared.

5.3. Communication and authentication

As established earlier in this document, the communication channels between CSIRT-FORENSICS and its clients are essentially two: email and telephone, the former being used as the main channel and for the exchange of information with a certain degree of confidentiality.

In the case of email, PGP keys will be used to sign messages and to encrypt information that, due to its level of confidentiality, must be protected.

The accounts used by CSIRT-FORENSICS and their associated PGP keys are as follows:

soc (at) forensic-security [dot] com Fingerprint: 1469 C680 3E62 0514 53F2 EE8E 2A96 7415 A52E 6142
consultas.soc (at) forensic-security [dot] com Fingerprint: 4143 510E 4FFB 460B 16D1 2C33 A606 B888 6726 7431 04D6

The telephone will be used without encryption, for communications in which the information exchanged has a low degree of confidentiality and therefore does not require special protection. This type of information may also be exchanged by email without using PGP key encryption.

6. Services

6.1. Vulnerability analysis and management

Management of the vulnerability lifecycle through continuous analysis of the configuration of our clients' infrastructure against known threats and vulnerabilities.

6.2. Event detection and analysis

Real-time monitoring, event correlation, analysis and notification of security incidents.

6.3. Incident response

Adds to the event detection and analysis service an additional layer of autonomy that makes it possible to minimize reaction times to a cyberattack or security incident.

6.4. Education and training

Simulation of customized phishing campaigns and analysis of user responses to such campaigns to assess our users' level of awareness regarding this type of attack. The service is complemented by training materials for users in order to improve their ability to notice such attacks.

6.5. Ethical hacking audits

In-depth analysis of vulnerabilities in the client's systems, where a cybersecurity expert attempts to access the systems by exploiting existing vulnerabilities and issues a detailed report.

6.6. Managed services

Our expert operational teams are available in those technological areas (systems, OSS, applications…) where the client wishes to partially or fully delegate the management of their infrastructure. In any of the aforementioned areas, the principle of Security by Design is applied in the development of the solution.

7. Incident reporting form

When a client detects a security event or incident, it will report it to CSIRT-FORENSICS via the soc (at) forensic-security [dot] com email address, as indicated in previous sections of this document. In the exchange of this information, the protection measures defined in the CSIRT-FORENSICS Information Management Procedure will be used, through the use of PGP keys. These measures will consider both the classification of the information and the agreements established with each client at the start of service delivery.

The email must include all available information from among those listed in the following table:

WHAT TO REPORT	DESCRIPTION
Subject	A sentence that generally describes the incident.
Description	Detailed description of what happened.
Affected Party	Indicate whether one or several users are affected.
Date and time of the incident	Indicate as precisely as possible when the incident occurred.
Date and time of the incident detection	Indicate as precisely as possible when the incident was detected.
Incident taxonomy classification	Possible classification of the incident based on the taxonomy described. This classification is defined in the Security Incident Management Procedure of CSIRT-FORENSICS and will be provided to each client via the channel agreed with each of them at the start of service delivery.
Impact categorization of the incident	Estimated impact on the entity, depending on the level of incident affectation. This categorization is defined in the Security Incident Management Procedure of CSIRT-FORENSICS and will be provided to each client via the channel agreed with each of them at the start of service delivery.
Resources affected	Indicate technical information on the number and type of assets affected by the incident, including as much information as possible from the following: • Number of affected computers, servers or devices • Hostname and IP address • Function of the system • Time zone

	• Hardware • Operative system • Affected software • Affected files • Security configuration • Protocol/port
Origin of the incident	Indicate the cause of the incident if known, for example, opening a suspicious file, connection of a USB device, access to a malicious website, etc.
Attachments	Include attachments that may provide information to help identify the cause of the problem or its resolution (screenshots, log files, emails, etc.).

8. Disclaimer

Although all precautions will be taken in preparing information, notifications and alerts, CSIRT-FORENSICS assumes no responsibility for errors or omissions, nor for any damages resulting from the use of the information provided in the course of its services.

9. PGP KEYS

9.1. SOC (AT) FORENSIC-SECURITY [DOT] COM

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGbZebIBEADh99SL/PBb6RmahIopVNTSCfbSSowQJLjDpX2LeFKXyrdVdqmI
ePCEQBJyyfDNLntVC7YrPTUgEOaQowPFt71LXDzq2Wt4IAuygaVQXhcq62y1ZbjD
MoavsT+8obM1YMlp5zF0XSpQCP31fS8gOi9s+7e2SV2WawiKT5ZK9yP2+TMK3DDS
Cgc+mmrSdHi6zWYoFWqX6vIhXBtzm7uCcBHA8xm0U9dJHapwUAGPXBhBoK+by1i4
uae1Vjls1t0jjB6OCVmG6ceFuRyouoT9wHRWZpIBRy8hxdAacrUT7ReUjbFIp61y
kRsZXb/XEWF11PJlpn4tEbs2LjbGq2m+R38WEusQY+uNq1McsRZ19kgEqIca+ngQ
ih4PRr2CgAtlaLakz3w3wUCLCW8/06MPsUwfhTYFSApyiRvoYFNqmnTcv/Qrs7rE
/QHZLgNN+Ddknv2ua0SdwyNMB1ermOKjM4f0H/gnudxloIt/d+G3l0TFburez6QX
UwSeLLZaGaxp74eATog8z0mTZjOP4fUs4Dp07hyGhk7AFPjUKESK/WxwDbVzN6Rp
10iO7lKP+ZKt+FjX0LLr8ex5B3xznyO7zPeILiiTAeQx4UhqnIwzXUuX32PAcWv9
8ABbcryYHjHF2Tp5srV7BDfDM0/hT/vRBG6TD4E9QFfbVyxsc1t6CDzKgwARAQAB
tEZTT0MgQCBGb3JlbnNpYyAmIFNlY3VyaXR5IChQdWJsaWMgU09DIFBHUCkgPHNv
Y0Bmb3JlbnNpYy1zZWN1cml0eS5jb20+iQJOBBMBCgA4FiEEFGnGgD5iBRRT8u6O
KpZ0FaUuYUIFAmbZebICGwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQKpZ0
FaUuYUIuqxAA1oNSqAaFFdie8z1DDbDyfUEaSrqKg/IobxYzz+GFQKUjpZh8kMX1
G9gYodPbY96w03cu53mJIiJm1bBmXv/GNBxJvi75QG824xwvVFYhv+dZ6hAOEffl
IXIVFaI6zFXCeH9cdmMtir6mQxRc7dj8c5SApgjyv/tCbWPmmduLcnKVwsIdDp2L
eUfa17L3Wvkw0ZPCedf5YPgJAH3D3qCe7iO8IcWIZ3/eUp/DazIvhJD5eUGlC0Va
Zarg4fLxudo/AxXjiwHeTjsZbsOrReKM9PZO2aiFSoqyOixxWUaZcNwb5KxxYYpN
f5WORpuF7uSDsGBq92EzRkNmMPeKffl/FDfXj4BiG/Dc/y9mIiYQTSgP1zxsg9De
GSU5x8xA5ERPk7JEwNkpZt0fW1nwszcaaRsm1kZJQpL7zGZTvW9mbgDGw/ktwXbO
/iTruAa9oW2dUQ2iDPr28qY8FxiI3py0dS6lDu3ukqzsrZodG+OSbhRjThX0sdv1
TMg1SgdRB5jl3jQSNv0X+7YWMUyu+r2c8LOjQ9a2KlRxtXuRItKS4kQLBogzEKB+
Ugh62kKWL09DR9xidZ5h7YxcPuZO6Z+ucTPwSSzWdrnWCNte2A4O6y+YiQYguVQ5
MdpCntSl6o1E8rYLY2EgiEIOn7ubpDK+uq6mXWq+axFV0ntP3f7vQl+5Ag0EZtl5
sgEQANvynRNsIR24+Vs7iah3lEDgnq07sGwXWpVcirS8ShigE0HKNXiififzqHiP
JfpNUoskexCuWN7P3SB6iuIW9QXhRdOZZaXxPqaxhwo9LphqsYNe8UgdzeyVdBuq
a4ffglKVmchxfh/pWPM7E3mayqBpydE2j49L35AETEfI0RztBAMROrNNznjZ54gt
Lkqg6WLfx6Ezq3TZ9DtNnLYWuGQbjHgXcx8bY/domp3F4F7Mcgq21odHeGPphPMf
ncLQ++R/oI8lSqSNY6N7ueNBOmhjnMoGgDqdmB/bNwGIgT4CDLivNeUwm69ApZ8V
BG9luol+tqMdpWDWYkFL5E6VWVG0FfyISqRCMXkzd4MxI/Jn2SeQDdMv1g33FxDS
J6FMvIQMBo02sg/rhuG2tj454GlDjtKd/4WI5S/4bYyxRI5psnobHzYFYLOHoPGp
QEG4PgQp7aF8kGrcazu4GaZ/m7Q0l+GJ+D/WpNWIdEJfhY48Wjmwf5BKk4M98Gjh
2MsiNG/At8NVdJqzqrqDzQoUbkyop9UyazwJS6gGJNLoR+zkktWuyy5lQ6sC9id8
etLRqlhauyvLjaROt6+oN+fAW+N+li274RmkpdpF085wQiJEcEW0EB2AP0AfLsry
CUYbEtGcohR+IFKxkMilSYH39GqVCxGstMEbbR2vrA9BOHrZABEBAAGJAjYEGAEK
ACAWIQQUacaAPmIFFFPy7o4qlnQVpS5hQgUCZtl5sgIbDAAKCRAqlnQVpS5hQlP7
D/4qTOS6ub1h/UUEV9W4C1vDY1f6YaHhdi82omFnTJ8WGo1+UCJ1tsUSlcbRG5Gt
ED3k22m+gu295+Yw7fRq2shtMnE1vbCrX/fnNK/7YAjKZWq5wB3W1R7RFCYt67Zn
njLlBIMM6ABY2p7yP/aoTfjnWXbQHHE7Tihm5gNHiLsLQTHPO+MWRRGZPheVpTlh
jTFoM4xRn+zmZNuLu2jpIGa9EZBfuHVEsETKChEVTr8BeUQvbTeAnjDiJEyPKskJ
WO4bxgkieOgVNuyVFkwfbsdfbsRrA0rWJ+mKi+IxH/ecUqP26k7uoGrSEUIYDl0W
/gCP6mkKunVW3qThOwNmaFcDWGNM9qBs2R/qW9IkM++iN6cjMT2XkUD34XqMWnMa
4JiMg52OSLTLtD+DQwZZuq/2MAp9UV5vypwcfqKxvAte7tse/CoGv5M26Jw03krB
6TtCmI3Jqhle9E4u4JMQRdwUbNS0/5Au28bLfF/GdtEcCFRE93ZlGOYeEiWIsoNv
Foa4ePfcYFGb3VsxeKtmXs/hz2TC3T9Wp4DoznnZbv1Kt06oYv7P2LX8+N7thHIF
DEoRoIijYaMbUaKrBIVD7bxDCIOTGEhPHxy5uLdOB90HOrKUMawRy3x2vzpW8PTZ
jjT6MWlewBp8EhCBK6/0SYMX7GVs5XybN4OA1qjfXMzjsQ==
=Phqi
-----END PGP PUBLIC KEY BLOCK-----
```

9.2. CONSULTAS.SOC (AT) FORENSIC-SECURITY [DOT] COM

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGbZxkIBEADCDsvZlcm8Ihs+s7933biPILUHazHUFqKhHfs1Q6IarQGUWh6w
KlMt7bxbxLZBEnzgWdEZwst0F/wmuot8VjsFXGB4jQCPCQlmu09xIuPKDhnc/KbX
CmA4aeUv+UdkYMN0gs4aUowZP0+1MYuGRydqATw6MSdUP7FG1nkuu0QuyiSMgLqn
RPaNVVxkzWERpClELigrNG2dUG8daQlF5LcZPoJD1SxqD2pBe+f9uQEDUUgxmfrn
VIoYT7SLooYUMbiM2knKLx0dtN656twRyl+vt9dmAY6JrzzAozbZI5eFp8HjthlE
C1taXN6/I/ibHJf2dCZ2phmP33MCt/vaS/cDBMb+tcCVENG1YRYfb/ciS2EbPWTs
03g1ZZqitwXKFibCJIND/H4GyBaXDx4CuuAkioavq6qsCzdvPfdLbWjxVlq0SIL2
uLP4cBbdfti6hFmWPfZaGzpbx8zYuiQP55v35bVNn2riWbt0B6mWVGInjh5TNgCt
JvyXs3SUhYzxN7Pm+e0CGTUxrsNaw0AhgZq6PHgJzrbiAmSGhhoCxLx3E44yPIUH
artJ58kj/txS2Un6HZKUn73BSpAU3Av6leWRkT79IXuRufKksKzM2EMnYXkJIE02
BranX+umI1PNo8q+NTP8n25++zOVN124/yh3dn+XG2ql6s/eV3jTGYvNVQARAQAB
tGRDb25zdWx0YXMgU09DIEAgRm9yZW5zaWMgJiBTZWN1cml0eSAoUHVibGljIENv
bnN1bHRhcyBTT0MgUEdQKSA8Y29uc3VsdGFzLnNvY0Bmb3JlbnNpYy1zZWN1cml0
eS5jb20+iQJUBBMBCgA+FiEEQUNRDk/7RgsW0Swzpga4iGcmdDEFAmbZxkICGwMF
CQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQpga4iGcmdDFO8w/+OsoL
ch5KqiZWkbnIdk1LX+ln1rUyU9RodeRx7I+WMshLb9msHsoeC9WT4iGsKaTp/3t2
ZtM506tZLJt9xMv9RwaBk+8uVROoCbviIWxsVtM8mtYPgfhNKu+9MALs8CR3NWIF
UTdxq1tOlQOA9BRx6pgnHqZHEwAtPvKQstWSvE4K8iaIm53voMIS1ehObV0NzHVK
avgHdohxVQi9wjDejoBgLRY3jj9LZXNG1+etL2ji6H/d14Xa8++mMOooF97EM+ci
44iRNPd+4/zCCbWpSBGjInrbdAnkM8MUl6dfJlXeTZyZShg3U7e5znwPol+HKvdW
t3LpL8LHZYR6j2MxEmUb95u3aGkbcR4GVoY7ejkUubSsEj/GXiHSP2gv2hfZcy/3
pO51idgviryX8p4QjTucOhjNss1C+qv4lSvcMcxYaglZ9kP/mr/t2tSIWv4rCXg9
I02SqWOBqQugYwcHEVmX0skKv4+Rc4DpK/WZoP/jhueQhlB4vcdvlqhUB/SZA3HS
ciskODQEBcCu7Tu3vchY7DiL1MkfqxIYAd16BHRtfUaoUwPLvJBi3aKmn62uMwiC
30ecx3S39tc/pF4ip39OPUTN54ncatWSAWMOu3FZUMhqmZZHQHNbpQ725/+RGwmY
SCP7OjkC4FhMOyw7JQ9fs0pzUd2Xigh2z5EEo3i5Ag0EZtnGQgEQALw/gdyOIdJp
Ffugj58wkMmpNRz4TohzGl6MtpCkHn8r7X2jm+LRXGwahLaZwVrLBbK/jUNNzQW2
i5m4N16Pi3JJb7MapGapiLfuGNHljWIQtYlfRQ+dVA+iQXuq3HygHyr7A1k5G+L3
02TWlL21DBSKNkhPogrOSut1kOaYyWWUmXbNeOheyS7qq2L0qjMuYIaDkz35JgFA
Nq27NdNwiyFBILX2t+Wh8y73xuS1H1C50tq3pckj7gEQjWcZn2sj9bDuBfCot+hP
39kHOqp4A9VyO7Kc37Lz3Trk4I7HfpmMP9oRBvol9BEu6fdmTBVJsMDltQwHTI8n
G+hFAx5WO/YRKbL2hrRqfyxd5OfM645Ve5FehL/xJlOhq29OG6LYEDBAequmoHx6
V82OhrNwqdk2chw4qT6w/21dG63Hr7WjBx9TISmQl9vUB87+EY38S/58iiNqeUqD
nwSuYigSPxxfnVcHzApxPABHORlPPAMQy0INhH0hPXBr+1Wf3uSEq5/B7m8EMkLS
hVQEeNq9uOlwhPw0s3UKszMKSxCMqHDYjBo5OCz+YbBBqO8LDessLqYrZODJ7bJh
bvu/7dsie4Py+QpuwDAjO+oiTS3OfWQ4PMNIloTx64Q4O+5qJCv6k+/qlkMP7GDo
kTdh74BHHKNDV+XAcLEJ5dowVYQwYB7PABEBAAGJAjwEGAEKACYWIQRBQ1EOT/tG
CxbRLDOmBriIZyZ0MQUCZtnGQgIbDAUJA8JnAAAKCRCmBriIZyZ0MTMmD/9pNTXj
ou9Wu70noRcS5hgBkl7CtJmEuz02ueR0jS2F0Uxqord9aghYs9AYdzCzgAXee0rM
kAZyByR63zt7dAOW70yKoQ0xMppvP6MUtbFJQ2pz2EM7vrCR+azJB+edLfHTrIAI
rOECp6DHa76yiVbX/+BjPiTK7Ds2/o/MHQClyRIrT0/t8RXtErkzW2QcxznqmPGw
1LwLsFVN2FL/DvvWTbr3XlaNRw+l/vLnlBMCLIoXfdSoxeEVHmzhuk6KQrkzqENO
bW/0ENG2wQ4u9NOWl1cJ230tLOkd+gxYnrDx/3kv+w9UQD8P7vsU7hYkWJhP56KR
EETy0vLCHHs4QInq0Ll5YExNcvesOWakaHY9/kJfkp1KmfOXo51ZEd8W52SNozkT
hDcTyhJQmOuu1AlPdMcSDZtQKTMq0taRHmPZctEcurETNVimIXqEuTMJQkZfRLJz
clRqPP7zPrz2QRLwakkvP0W7Mq9hXAs0sOvRZk2TdeizMvwTm+WT00dTi8+jVCF1
HwZ+FL18ISJVgfdk5dV6EX3iGJNKQ3lN9Mx85NUoPi0L9Mpw1vBQZRQLIbEQYlH2
XAi80cpcXD62mQTAEV2UmYjHLdq/L5hKOGNGrjfHGfUvhwQpF5r3gTNsKgr9Zb6N
LIs1e5oKCy6wZhuQws0s/1HEfliiif0BnAgGHQ==
=6gU2
-----END PGP PUBLIC KEY BLOCK-----
```