2. Organization

cyber_Folks S.A.
ul. Franklina Roosevelta 22, 60-829 Poznan
tel.: (+48) 12 296 36 63, fax: (+48) 12 395 33 65
hotline / infolinia: (+48) 501 DOMENY (366 369)
support@certyfikatyssl.pl , www.certyfikatyssl.pl , www.domeny.pl

1. ORGANIZATION
CYBER_FOLKS S.A., registered in Poland, operates worldwide, with separate operations, research & development and server operation sites. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

1.1. CONFORMANCE TO THIS CPS
CYBER_FOLKS S.A. conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

1.2. TERMINATION OF CA'S OPERATIONS
In case of termination of CA operations for any reason whatsoever, CYBER_FOLKS S.A. will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, CYBER_FOLKS S.A. will take the following steps, where possible:
- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as CYBER_FOLKS S.A.'s.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

1.3. FORM OF RECORDS
CYBER_FOLKS S.A. retains records in electronic or in paper-based format for a period detailed in this CPS. CYBER_FOLKS S.A. may require subscribers to submit appropriate documentation in support of a certificate application.

1.4. RECORDS RETENTION PERIOD
CYBER_FOLKS S.A. retains the records of CYBER_FOLKS S.A. digital certificates and the associated documentation for a term of than 7 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation.

Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that CYBER_FOLKS S.A. may see fit.

Such records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

1.5. LOGS FOR CORE FUNCTIONS

For audit purposes, CYBER_FOLKS S.A. maintains electronic or manual logs of the following events for core functions. All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by CYBER_FOLKS S.A. staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived. All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

1.5.1. CA & CERTIFICATE LIFECYCLE MANAGEMENT

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals
- Subscriber certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Custody of keys and of devices and media holding keys
- Compromise of a private key

1.5.2. SECURITY RELATED EVENTS

- System downtime, software crashes and hardware failures
- CA system actions performed by CYBER_FOLKS S.A. personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, deinstallation, service or repair and retirement
- Successful and unsuccessful CYBER_FOLKS S.A. PKI access attempts
- Secure CA facility visitor entry and exit

1.5.3. CERTIFICATE APPLICATION INFORMATION

- The documentation and other related information presented by the applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

1.6. BUSINESS CONTINUITY PLANS AND DISASTER RECOVERY

CYBER_FOLKS S.A. undertakes all the steps necessary to provide continuity and /or recovery of providing of services governed by this CPS. These steps include creation of backups of relevant electronic data.

1.7. AVAILABILITY OF REVOCATION DATA
CYBER_FOLKS S.A. allows access to Certificate Revocation Lists (CRLs) and to OCSP (Online Certificate Status Protocol).

1.8. PUBLICATION OF CRITICAL INFORMATION
CYBER_FOLKS S.A. publishes this CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official CYBER_FOLKS S.A. repository at https://www.certyfikatyssl.pl/repository. The CYBER_FOLKS S.A. Certificate Policy Authority maintains the CYBER_FOLKS S.A. repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this CPS.

1.9. CONFIDENTIAL INFORMATION
CYBER_FOLKS S.A. observes applicable rules on the protection of personal data deemed by law or the CYBER_FOLKS S.A. privacy policy to be confidential.

1.9.1. TYPES OF INFORMATION DEEMED AS CONFIDENTIAL
Domeny.pl keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.
• Subscriber agreements.
• Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
• Transaction records and financial audit records.
• External or internal audit trail records and reports,
• Contingency plans and disaster recovery plans.
• Internal tracks and records on the operations of CYBER_FOLKS S.A. infrastructure, certificate management and enrolment services and data.

1.9.2. TYPES OF INFORMATION NOT DEEMED AS CONFIDENTIAL
Subscribers acknowledge that revocation data of all certificates issued by the CYBER_FOLKS S.A. CA is public information is published every 24 hours. Subscriber application data marked as "Public" in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with this CPS.

1.9.3. ACCESS TO CONFIDENTIAL INFORMATION
All personnel in trusted positions handle all information in strict confidence, complying with the requirements of the Polish and European law on the protection of personal data.

1.9.4. RELEASE OF CONFIDENTIAL INFORMATION
CYBER_FOLKS S.A. is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying jointly:
• The party to whom CYBER_FOLKS S.A. owes a duty to keep information confidential.
• The party requesting such information.
• A court or other competent authority order.

1.10. PERSONNEL MANAGEMENT AND PRACTICES

Consistent with this CPS CYBER_FOLKS S.A. follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties, according to the norm ISO/IEC 27001:2005.

1.10.1. TRUSTED ROLES

Trusted roles relate to access to the CYBER_FOLKS S.A. account management system, with functional permissions applied on an individual basis. Senior members of the management team decide permissions, with signed authorizations being archived.

Trusted personnel must identify and authenticate themselves to the system before access is granted. Identification is via a username, with authentication requiring a password and digital certificate.

1.10.2. PERSONNEL CONTROLS

All trusted personnel have background checks before access is granted to CYBER_FOLKS S.A.'s systems according to the norm ISO/IEC 27001:2005.

1.11. PRIVACY POLICY

CYBER_FOLKS S.A. has implemented a privacy policy, which complies with this CPS. The CYBER_FOLKS S.A. privacy policy is published at the Domeny.pl repository at https://www.certyfikatyssl.pl/repository.

1.12. PUBLICATION INFORMATION

The CYBER_FOLKS S.A. certificate services and the CYBER_FOLKS S.A. repository are accessible through several means of communication:

• On the web: https://www.certyfikatyssl.pl/repository

• By email from bok@domeny.pl

• and by mail from:

cyber_Folks S.A.

ul. Franklina Roosevelta 22

60-829 Poznań