# NIST TECH AND OPS MEASURES

## RELATED TO FIPS 140-2 ENCRYPTION

Federal Information Processing Standards 140-2 Encryption
Cryptographic Module Validation Program
Computer Security Resource Center
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce

AND

Federal Information Processing Standards 140-2 Encryption
Canadian Centre for Cyber Security
Canadian FIPS 140-2 Cryptographic Module Validation Authority
Government of Canada

**RPost´s main responsibilities as a data processor are to provide for the confidentiality, integrity, availability, and resilience of systems and services that process sensitive business, government, and personal (“Protected”) data.**

**This document outlines the technical and organizational measures that RPost has implemented to comply with legal and contractual security obligations while processing Protected data. These measures apply to all data processing activities that are within the control of RPost.**

### 1. Transfer and Dissemination Control

RPost systems are built to protect Protected data and to secure transfer of Protected data.

Data in transit that is designated to be sent securely is protected using RSA-AES256, PDF-AES256 or TLS encryption. All system stored data is encrypted at rest. The storage volumes are encrypted at block level using AES-256 in a manner consistent with NIST 800-57 and with FIPS 140-2 approved algorithms.

Two-factor authentication is required for elevated and privileged access to all critical systems and environments. Access is only granted to authorized people using VPN connections.

Mechanisms for securing data transfer, for monitoring and for logging activities in networks have been established to the required extent.

Systems are protected from malicious and vulnerable sites. Network and systems follow CIS hardening benchmarks, only certain systems have access to internet while the rest of the systems can only access internal systems. Firewalls and intrusion detection and prevention systems (IDS / IPS) are in place.

To minimize the risk of data breaches, paper printouts and exports of confidential data are avoided whenever possible.

Electronic data exports that are no longer required are deleted from the respective storage locations.

## 2. Cryptographic Module Control & NIST FIPS 140-2 Encryption

The National Institute of Standards and Technology (NIST), as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security (CCCS), as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; have validated the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

RPost services use cryptographic modules maintained by third parties publish validated certification with NIST and CCCS Federal Information Processing Standards 140-2 Encryption.

More specifically,

- RPost's message-level encryption within its RMail®, Registered Email™, and RDocs™ services use in components RSA-AES-256-bit encryption generated by a component of the RMail® and Registered Email™ processing servers, that component being Software Module: **Cryptographic Primitives Library** *(Microsoft)* with CMVP Certificate #4356.

- RPost's message-level encryption within its RMail®, Registered Email™ and RDocs™ services additionally use PDF-AES-256-bit encryption generated by a component of the RMail® and Registered Email™ processing servers, that component being Software Module: **BC-FNA** *(Bouncy Castle FIPS .NET API)* with CMVP Certificate #4416.

- RPost internal processing system stored data within all RPost services is encrypted at rest using RPost managed and frequently rotated keys within the AWS Key Management Service (KMS). AWS KMS uses configurable cryptographic algorithms so that the system can quickly migrate from one approved algorithm, or mode, to another. The initial default set of cryptographic algorithms has been selected from Federal Information Processing Standard (FIPS-approved) algorithms for their security properties and performance. AWS KMS key generation is performed on the AWS KMS HSMs. The HSMs implement a hybrid random number generator that uses the NIST SP800-90A Deterministic Random Bit Generator (DRBG) CTR_DRBG using AES-256. It is seeded with a nondeterministic random bit generator with 384-bits of entropy and updated with additional entropy to provide prediction resistance on every call for cryptographic material. The storage volumes are encrypted at block level using these FIPS 140-2 approved algorithms, Hardware Module: **AWS Key Management Service HSM** *(Amazon Web Services)* with CMVP Certificate #4523.

- RPost electronic signature service records and message level encryption message body text parts are secured for content integrity and origination using X.509 public key digital certificates, that are AATL recognized DigiCert Trusted G4 Code Signing RSA4096 SHA384 digital certificates.

- RPost transmission level encryption within its RMail®, Registered Email™, RDocs™, RSign®, and RForms™ services use X.509v3 RSA Encryption for TLS transmission through TLS 1.3. For RMail and Registered Email encryption services, the sender organization can enforce either AES-256-bit encryption using the modules noted above or X.509v3 RSA Encryption Transport Layer Security (TLS) 1.2 or TLS 1.3 transmission encryption and if the receiving server cannot accommodate such, automatically revert to AES-256-bit encryption using the modules noted above. The decision to enforce AES-256-bit message level encryption or a particular minimum TLS level is set by the customer administrator in the RPost RPortal customer settings application. The X.509v3 RSA Encryption certificate is issued by Let's Encrypt with a Certification Practice Statement (CPS) posted according to the Internet Security Research Group (ISRG) published operating practices. A certificate sample reference from one of the RPost system server mail transport agents is below:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:45:d7:68:35:59:23:42:c4:ee:fa:ab:00:cc:17:ca:23:66
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Aug 15 11:41:32 2023 GMT
            Not After : Nov 13 11:41:31 2023 GMT
        Subject: CN = mta21.r1.rpost.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ed:a8:29:3b:1d:8c:f1:40:b7:3f:0e:2f:03:42:
                    d6:a7:68:df:34:a3:5c:1c:37:23:fe:da:22:1d:4e:
                    7d:b6:83:ae:8e:e7:8f:d9:c8:35:7b:e0:b0:42:c6:
                    95:15:71:7f:a2:23:7f:35:d6:e3:d3:09:d8:d9:fe:
                    fc:82:96:d0:25:cf:74:98:0a:b7:a8:31:f9:60:82:
                    68:93:4d:09:07:6a:7b:21:4b:d5:01:f0:c0:7e:ef:
                    f6:49:1f:f3:46:b4:cf:a5:ab:0a:2e:9a:af:91:59:
                    40:06:e1:ea:ea:9b:88:b1:8a:09:a0:19:a3:ff:35:
                    a7:df:36:ca:46:bb:66:39:f7:0d:c7:cd:06:1d:8d:
                    2c:31:c3:54:57:f2:51:59:22:63:a7:41:c7:a1:2e:
                    3e:aa:c7:2f:10:55:9e:18:75:4c:b8:46:16:87:7c:
                    4b:ef:55:5e:00:88:71:ca:86:0c:76:5c:38:61:14:
                    ff:2f:ce:21:ee:4b:96:d7:d6:ad:4a:08:6f:66:20:
                    c6:ad:b4:ce:20:9d:18:c6:34:1f:4c:f0:01:b2:7c:
                    40:78:b8:be:ad:fb:5c:5b:1b:17:a9:1a:12:64:3f:
                    f6:ab:4f:6e:fe:6f:b6:0b:9c:4b:3e:b9:96:26:20:
                    4d:22:a6:05:31:83:f2:5c:4d:8b:bc:50:85:c4:82:
                    a8:b5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                E6:F7:10:A1:22:91:1F:08:0B:54:A1:2D:F8:5A:67:A9:9F:6B:00:0C
            X509v3 Authority Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
            Authority Information Access:
                OCSP - URI:http://r3.o.lencr.org
                CA Issuers - URI:http://r3.i.lencr.org/
            X509v3 Subject Alternative Name:
                DNS:mta21.r1.rpost.net
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : B7:3E:FB:24:DF:9C:4D:BA:75:F2:39:C5:BA:58:F4:6C:
                                5D:FC:42:CF:7A:9F:35:C4:9E:1D:09:81:25:ED:B4:99
                    Timestamp : Aug 15 12:41:32.429 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:69:71:A2:AD:F2:E7:47:C0:C4:D0:9C:AE:
                                E7:0C:5C:39:29:49:84:7A:00:7F:D0:65:3D:28:46:E1:
                                C0:71:DA:34:02:21:00:C8:8E:30:E7:4E:3B:81:AF:38:
                                A6:AE:9C:5D:AE:9A:40:09:CB:FA:70:BF:04:88:77:CD:
                                DC:26:6A:3D:9A:EF:88
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : E8:3E:D0:DA:3E:F5:06:35:32:E7:57:28:BC:89:6B:C9:
                                03:D3:CB:D1:11:6B:EC:EB:69:E1:77:7D:6D:06:BD:6E
                    Timestamp : Aug 15 12:41:32.437 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:A1:FA:6B:73:66:A7:33:32:30:52:CD:
                                CF:BB:C0:E6:FA:CF:4F:B3:6A:89:C4:B7:67:86:A0:85:
                                76:51:B2:BB:A0:02:21:00:D8:47:98:EA:94:49:79:8C:
                                0B:DF:72:49:6A:F0:AD:23:FA:AF:49:3E:25:99:8A:61:
                                09:5B:9D:8E:09:A9:41:CA
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        84:9b:71:90:36:25:55:1e:f9:c6:15:9b:53:58:f0:0a:5a:4d:
        4e:bc:a1:fb:32:1e:6d:4d:f3:89:23:a4:c8:af:36:e5:d0:0e:
        fd:36:10:f8:90:1f:66:dc:c1:a9:6c:ae:be:2e:dc:33:f2:a8:
        ca:56:b9:89:6d:c6:04:e0:c5:21:46:76:e4:ab:86:b7:fc:a0:
        64:65:22:12:05:22:3e:7f:51:16:07:95:b9:1e:ab:df:c0:ef:
        2b:8f:a8:20:6a:38:a4:52:46:28:4e:c5:d5:e4:97:af:fd:bd:
        cf:40:ce:2c:a3:12:b8:c1:c6:15:1b:17:08:fe:4d:3a:c9:e7:
        d6:f1:0a:b9:2d:b9:04:f9:f3:74:6b:3d:17:d6:13:ad:4d:2b:
        cb:63:ec:83:14:9c:6f:ef:56:bd:79:9b:c3:90:fb:b1:71:58:
        54:41:5b:2f:8e:09:bc:b7:bd:65:7f:f2:40:04:f5:ba:16:33:
        ac:96:6e:22:cd:05:fe:50:b2:4b:15:69:a4:56:5b:7f:ea:5e:
        fe:fa:20:88:e2:aa:bc:75:08:c6:58:7a:44:6b:e8:fc:4d:d6:
        46:ab:43:3d:db:72:9b:2b:19:a2:2a:6a:f8:b1:8a:49:59:91:
        e4:97:89:f6:83:da:ad:7c:2e:57:7f:df:39:0a:08:7e:7f:5c:
        83:9f:28:36
notBefore=Aug 15 11:41:32 2023 GMT
notAfter=Nov 13 11:41:31 2023 GMT
```

## 3. Access Control

Access rights to IT systems, data and physical buildings are provided following the need-to-know, least privilege and role-based segregation principles, employees and third-party users are only granted the level of access strictly necessary to perform their activities.

Access rights are reviewed regularly and those that are no longer required are withdrawn periodically.

User access logging mechanisms are in place, both for the RPost applications and for internal systems.

Data of a client´s instance is logically isolated from data of other customers at a database level.

## 4. Physical access control

Physical secure areas are defined based on information security and data protection requirements. These areas are safeguarded against unauthorized access using appropriate physical security measures, such as personalized access media, video surveillance, and alarm systems.

To prevent unauthorized persons from accessing security areas, procedures are in place to manage visitors and deliveries.

All regular RPost employees are issued a key to gain access to office working environment facilities. All lost or stolen keys must be reported to one's supervisor as soon as possible. These keys do not provide access to any secure rooms, server rooms, or production service operational facilities.

Upon separation from RPost, and at any other time upon RPost's request, all keys must be returned to the supervisor.

## 5. Logical Access Control to Processing Systems

All data processing systems, information systems, applications and databases are password protected following policies that enforce the use of complex passwords.

Passwords must be periodically updated and changed whenever there is an indication that the password has been compromised.

Access to production environments and data is logged and restricted to selected designated technology resources, and production and non-production environments are logically separated.

Access to information is provided considering the need-to-know principle. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives. Approvals are managed by workflow tools that maintain audit records of changes.

Special procedures are in place for granting access rights to privileged systems. Two-factor authentication is required for elevated and privileged access to all critical systems, this includes Developer, QA, Preview/Staging and Production environments. In summary:

- Access is limited to designated people in the company.
- Authorized people access the environments using VPN connection.
- They are required to enter username and password in the first step.
- Once authenticated, they are required to enter a passcode from an authenticator app preconfigured on their mobile devices or other or multi-factor process.

To maintain information security, it is mandatory to lock computers (screen lock - password protected) when leaving the workplace. The screen lock must be set-up to be automatically activated after a short duration of inactivity.

### 6. User Activity Control

Employees must be periodically provided with basic information security and data privacy training by attending weekly RStaff training sessions. Training is also part of new hire orientation. Attendance in these RStaff training sessions are tracked per team member. These weekly meetings provide advice and training on security concepts.

User activities, including logon attempts to data processing IT systems, are logged.

Administrative activities on IT systems, such as configuration changes, are logged.

Configuration files are regularly backed up, checked, and a history is kept.

### 7. Segregation Control

Multitenant systems are used, or systems are physically or logically separated to ensure that personal data collected for different purposes are not mixed in their processing.

### 8. Data Carrier and Mobile Device Control

No client personal data is transmitted, in the course of normal business, to be stored on smartphones or USB sticks, and if any transmission to such is required, it is required to be transmitted securely.

System electronic storage media that are no longer required will be securely disposed of or destroyed in a way that makes it impossible to retrieve or access the stored data.

### 9. Pseudonymization and Anonymization

Pseudonymization or anonymization is applied to personal data to the extent necessary or at the option of the user.

In development environments used for testing purposes, data is anonymized or pseudonymized wherever possible.

Data analyzed to generate usage statistics is anonymized to protect the privacy of the data subjects.

### 10. Input Control

Mechanisms for subsequent verification of who performed data entry, changes, or delete operations are in place to the required extent. Log information is stored securely and protected from tampering, ensuring the integrity of the information.

### 11. Availability Control, Resilience and Recoverability

A Disaster Recovery and Business Continuity plan is in place and defines measures intended to ensure that personal data is protected against accidental destruction or loss. It is based on a redundant design of communication, data processing systems and supporting facilities, including failover, data replication, load balancing and periodic backups. Additionally, the datacenters that host the RPost infrastructure follow the best industry standards when it comes to hardening and physical protection, high-availability internet connection, redundancy of storage, power and network.

The Disaster Recovery and Business Continuity plan is periodically reviewed, both internally and by external vendors upon request.

Appropriate virus protection is in place related to email communications services.

## 12. Job Control and Subcontracting

When selecting subcontractors, a main objective is to minimize the risk of non-compliance with data protection objectives. The selection follows a well stablished vendor qualification and management process designed to include, between other key points, a thorough evaluation of potential subcontractors' technical and organizational measures to ensure they are capable of safeguarding personal data to the required standard. The subcontractors are also required to comply with the data protection policies and regulations in force.

## 13. Review, Assessment and Evaluation

Periodically assessments are in place on IT systems for potential technical vulnerabilities or errors. Once identified, appropriate measures are taken in a timely manner to mitigate them, this includes deploying critical patches for both operating systems and software applications.

Platform and technology upgrades are periodically performed by reviewing used third party software and assuring the most recent, stable, and secure versions are installed.

All changes and configurations updates are properly documented, reviewed, approved after impact analysis, applied in test environments first, tested to ensure that they are functioning properly, and finally rolled out to production systems.

Internal and external reviews of system, processes, IT security, data protection, and controls, are in place.

*Last Modified August 29, 2023*