THOMPSON RIVERS UNIVERSITY

# TRU DATA SECURITY SCHEDULE

## Definitions

1. In this Schedule:

   (a) "**Contractor Personnel**" means all individuals hired or used by the Contractor or any Subcontractor to perform the Contractor's obligations under this Agreement.

   (b) "**Contractor Systems**" means any systems, subsystems, equipment, devices, infrastructure, networks, hardware or software (including application programming interfaces) used in connection with the Services that are not TRU Systems.

   (c) "**Incident**" means an information incident, a security breach or an incident that affects, has affected, or may affect, the confidentiality, integrity or availability of TRU Information, or the continuity or security of TRU Systems or Contractor Systems.

   (d) "**Industry Best Practice**" means commonly accepted industry norms that a prudent operator providing services similar to the Services would implement.

   (e) "**TRU Information**" means any information, including any "personal information", as defined in the Privacy Protection Schedule, data, or records provided by or on behalf of TRU in connection with this Agreement that is disclosed to the Contractor, accessed by the Contractor or collected by the Contractor in relation to the Services and includes any information derived from such information.

   (f) "**TRU Systems**" means any systems, subsystems, equipment, devices, infrastructure, networks, hardware or software (including application programming interfaces) made available to the Contractor by TRU in connection with this Agreement.

## Interpretation and Applicability

2. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
3. In this Schedule, references to Services includes, if applicable, any cloud services used by the Contractor to deliver the Services.
4. Unless otherwise specified in this Agreement, the terms and conditions of this Schedule apply to the provision of all Services.
5. Any reference to the Contractor in this Schedule will include all Contractor Personnel, as applicable.

## Expectation of Standards

6. The Contractor must ensure that its Contractor Personnel involved in the provisions of the Services meet or exceed the standards set forth in this Schedule.

## Industry Best Practice

7. The Contractor must have in place and maintain security controls to protect TRU Information that conform to Industry Best Practice and perform its obligation under this Schedule in a manner that best conforms to Industry Best Practice.

## Compliance and Certifications

8. The Contractor must:
   (a) maintain ISO/IEC 27001 certification based on IT controls in ISO/IEC 27002; or SOC 2 Type 2 compliance; or
   (b) comply with applicable Province of British Columbia IM/IT standards accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards.

9. If any cloud services are used by the Contractor in connection with the delivery of the Services, the Contractor must maintain at least one of the following:
   (a) compliance with the Canadian Centre for Cyber Security Medium Cloud Control Profile at https://www.cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103
   (b) compliance with requirements identified for a provider of cloud services in the US Federal Risk and Authorization Management Program (FedRAMP) for moderate impact information systems
   (c) ISO/IEC 27001 certification based on requirements in ISO/IEC 27002 and ISO/IEC 27017; or SOC 2 type 2 compliance; or
   (d) Cloud Security Alliance (CSA) – Level 2 CSA STAR certification.

**Attestation of Compliance and Certification of Services**

10. The Contractor must provide TRU with evidence satisfactory to TRU, including any available independent third-party attestations, to verify all applicable compliance requirements described in sections 8 and 9.
11. If applicable, must provide a PA-DSS certification and/or proof of PCI/DSS compliance.

**Access Control**

12. Where the Contractor manages access to any systems that contain TRU Information, the Contractor must:
   (a) use globally accepted access control mechanisms and practices that comply with Industry Best Practices
   (b) grant access only to Contractor Personnel as required for such Contractor Personnel to perform the applicable Services, and only for the duration required to perform such Services
   (c) implement access control policies and procedures that address onboarding, offboarding, job role changes, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts
   (d) identify and segregate conflicting duties and areas of responsibility to ensure separation of duties
   (e) maintain a current and accurate inventory of all accounts
   (f) review the inventory of all accounts on a regular basis to identify dormant, fictitious or unused accounts
   (g) enforce principles of “least privilege” and “need to know”
   (h) review account access rights on a regular basis to identify excessive privileges and promptly revoke any such privileges; and
   (i) enforce a limit of logon attempts and concurrent sessions.

**Authentication**

13. Where the Contractor manages account authentication controls for Contractor Personnel, the Contractor must:
   (a) use globally accepted authentication mechanisms and practices that comply with Industry Best Practices
   (b) require affected authentication credentials to be immediately changed when:
      (i) an account is suspected or confirmed to have been compromised,
      (ii) an account is authenticating for the first time, or
      (iii) the account’s authentication credential has been reset by an administrator
   (c) require multi-factor authentication for privileged access; and
   (d) require multi-factor authentication when accessing TRU Information records or administrative functions from untrusted networks.

**Security Awareness**

14. The Contractor must ensure that all Contractor Personnel complete security awareness training annually.

**Log Generation and Retention**

15. With respect to Contractor Systems, the Contractor must:
    (a) generate and, for a minimum period of 90 days, retain logs that are sufficiently detailed to determine who did what and when
    (b) provide TRU with timely access to logs upon written request by TRU
    (c) have the technical capability to forward the logs to TRU
    (d) correlate and monitor logs to detect and alert on any malicious activity
    (e) use a reliable time source to ensure accurate time stamps for the log entries; and
    (f) protect logs from loss, unauthorized access and tampering.

**Investigations Support and Security Investigations**

16. The Contractor must:
    (a) upon written request by TRU, provide reasonable investigative support to TRU, including e-discovery
    (b) maintain chain of custody for evidence
    (c) maintain any legal holds as requested by TRU
    (d) notify TRU in writing of any third-party investigation or request for TRU Information, and provide reasonable assistance to TRU to protect TRU Information; and
    (e) retain investigation reports related to a security investigation for a period of two (2) years after the investigation is complete or provide to TRU for retention.

**Development, Configuration and Vulnerability Management**

17. With respect to securing Contractor Systems, the Contractor must:
    (a) have an information security policy based on Industry Best Practices
    (b) apply system hardening methods
    (c) use Industry Best Practices when developing applications and application programming interfaces
    (d) secure all Contractor Systems with anti-malware protection
    (e) remedy vulnerabilities in a timely manner according to severity levels
    (f) patch all systems and software regularly according to Industry Best Practices
    (g) conduct static testing of the source code and configurations at scheduled intervals and before each release to identify known vulnerabilities
    (h) conduct dynamic testing at scheduled intervals and before each release to identify known vulnerabilities; and
    (i) conduct penetration tests at least annually.

**Business Continuity, Disaster Recovery and Backup Plans**

18. The Contractor must:
    (a) have business continuity and disaster recovery plans
    (b) conduct backups at scheduled intervals; and
    (c) review and test business continuity, disaster recovery, and backup plans and test procedures as set out in such plans annually.

**Incident Response and Management**

19. The Contractor must:
    (a) have incident management and incident response plans; and
    (b) review and test both incident management and incident response plans and test procedures set out in such plans annually.

**Notifications of Incidents**

20. The Contractor must notify TRU within 24 hours of the Contractor's identification of an Incident that has affected, or may affect, TRU Information.

**Notification of Changes**

21. The Contractor must immediately notify TRU of any changes to the Contractor Systems, Contractor's security policies, procedures or agreements that may materially lower the security of TRU Information.

**Asset Management and Disposal**

22. The Contractor must:
    (a) not use TRU Information for test or development purposes without the prior written approval of TRU
    (b) provide TRU, within 60 days following either a request by TRU or the date of expiration of the Agreement or earlier termination of the Services, with TRU Information in a secure format and form acceptable to TRU
    (c) maintain an inventory of TRU Information records
    (d) not use any hardware or software that are irreparable or at end of life
    (e) following receipt by TRU of TRU Information pursuant to section 21(b), securely dispose of TRU Information records using secure methods:
        (i) within 80 days following the expiration of the Agreement or earlier termination of the Services, or
        (ii) upon request by TRU in writing, and
    (f) maintain records of TRU Information record disposal for a period of 90 days following such disposal.

**Physical Security**

23. The Contractor must in relation to the Services:
    (a) develop, document, and disseminate a physical and environmental security protection policy and procedures
    (b) regularly review and update its current physical and environmental security protection policy and procedures; and
    (c) review the physical access logs for the facilities where the Contractor Systems are located at least monthly, when applicable.

**Threat and Risk Assessments**

24. The Contractor must in relation to the Services:
    (a) conduct threat and risk assessments on any part of the Contractor Systems that is new, or has been materially changed, and address the findings of such assessments since the last threat and risk assessment was conducted; and
    (b) support TRU in completing its security threat and risk assessments and address the findings of such assessments.

**Security Screening**

25. The Contractor must:
    (a) screen all Contractor Personnel prior to the Contractor authorizing access to TRU Information, TRU Systems, or Contractor Systems
    (b) conduct criminal record checks on all Contractor Personnel who will have access to any TRU Information, TRU Systems, or Contractor Systems prior to authorizing Contractor Personnel access to any TRU Information, TRU Systems, or Contractor Systems
    (c) make a reasonable determination on whether any Contractor Personnel presents an accepted security risk taking into consideration the duties of that Contractor Personnel, the type and sensitivity of information to which that Contractor Personnel may be exposed, applicable TRU IM/IT standards, and all applicable laws; and
    (d) require all Contractor Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable laws.

**Encryption**

26. The Contractor must:
    (a) always encrypt TRU Information while at rest and in transit
    (b) offer TRU the technical capability for cryptographic key management to allow TRU to manage encryption keys used to encrypt TRU Information at rest
    (c) not hold or have access to encryption keys if such encryption keys are managed by TRU to encrypt TRU information at rest or in transit; and
    (d) not provide any third party:
        (i) the encryption keys used to secure TRU Information, or
        (ii) with the ability to break the encryption used to secure TRU Information.

**Isolation Controls and Isolation of Data**

27. The Contractor must:
    (a) implement and maintain the logical or physical isolation of TRU Information
    (b) implement, where supported by available technology, the logical or physical isolation of audit records related to TRU Information and activities in connection with the Services; and
    (c) isolate management traffic into a separate network.

**Network Controls**

28. The Contractor must:
    (a) implement applicable security controls and other technical measures to protect and control traffic flow to and from the Contractor Systems; and
    (b) secure remote access to the Contractor Systems by all Contractor Personnel.

**Use of TRU Systems**

29. Use of TRU Systems by the Contractor or any Contractor Personnel must be restricted to activities necessary to perform the Services. TRU reserves the right to not make any TRU System or facility available to the Contractor unless the Contractor or Contractor Personnel (as applicable) agrees to any additional terms and conditions acceptable to TRU.

**Security Contact**

30. If not set out elsewhere in this Agreement, the Contractor must provide the contact information for the individual who will coordinate compliance by the Contractor on matters relating to this Schedule.

**Record Keeping**

31. The Contractor must keep records of every Incident that required notification pursuant to section 19.

**Survival**

The obligations of the Contractor set out in this Schedule will survive the termination of this Agreement.