University of Victoria | University Systems

University of Victoria Cloud Security Standard

Last Updated: August 27, 2018

Introduction

This Cloud Security Standard provides the list of controls that are required to secure Cloud Services to level of security congruent with the University of Victoria (UVic) Information Security Policy. This standard provides a list of security controls to protect faculty, staff, student, and operational data to be stored with a Cloud Service. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

The security controls presented in this standard are taken from the international best practice for cloud security and have been tailored for UVic suitability.

Purpose

The purpose of this document is to enable project teams to work with a defined set of security requirements which enable solutions to be developed, deployed and managed to UVic security standards, which are based upon international best practice for cloud deployments.

The controls have been presented as a SECURITY SCHEDULE so that they can be added as an addendum to a contract for Cloud Services. However, it is likely that a Cloud Service provider will have their own set of controls and policies and that that SECURITY SCHEDULE will be used as a baseline.

Cloud Service Providers (CSPs) will likely utilize other CSPs to provide much of the infrastructure used in their service offering. It is not sufficient for a CSP to simply cite the available security controls of their CSP; they must indicate and explain how they utilize these controls to handle UVic data. For example, a CSP may provide encryption but it must be enabled and encryption keys much be managed.

Critical Controls

All of the controls identified are important; removing one increases the probability and/or impact of a risk. These risks must be identified, mitigated using alternate methods if possible, and any residual risks remaining must be documented and accepted by the appropriate UVic Administrative Authority.

The following controls are the most critical in terms of risks:

1) **Security framework compliance and security controls attestation:** we rely on third-party attestation that a Cloud Service is adhering to established cloud security frameworks.
2) **Enable security investigations through accurate logging:** our own policies require us to be able to investigate violations and logging provides the necessary evidence to conduct this investigations.
3) **Detect, investigate, and report Information Incidents:** we have statutory and fiduciary obligations regarding data breaches and CSPs must assist us in meeting these obligations.
4) **Access control and account management standards:** these are fundamental controls to protect data in an information system from unauthorized access.
5) **Encryption standards:** these are fundamental controls to reduce the impact of a data breach.

SCHEDULE B

SECURITY SCHEDULE

This Schedule forms part of the agreement between the University of Victoria ("UVic") and _____ (the "Contractor") respecting RFP ___, (the "Agreement").

Definitions

1. In this Schedule,

(a) "**Act**" means the Freedom of Information and Protection of Privacy Act (British Columbia), as amended from time to time;

(b) "**Backup Policy**" means a pre-defined and scheduled process whereby all Cloud Service Customer Information from Cloud Service is copied to disk or other media to ensure complete recoverability in the event of accidental data deletion, corrupted information, or a system outage;

(c) "**Business Continuity Plan**" means the preparation and testing of measures that all protect Cloud Service Customer Information and provides the means for the recovery of Cloud Service and Cloud Service Customer Information in the event of any loss, damage or failure of Cloud Service Infrastructure;

(d) "**Cloud Service**" is a hosted service as set out in the Services Schedule and includes but is not limited to Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) services offered by the Cloud Service Provider that may or may not have components that are hosted at the University of Victoria;

(e) "**Cloud Service Customer**" means University of Victoria (UVic);

(f) "**Cloud Service Customer Information**" means all UVic data transferred into the Cloud Service by CSP or UVic data input in the production Cloud Service after launch, including all UVic information. This also includes all Security Event Logs generated by the Cloud Service.

(g) "**Cloud Service Provider**" ("**CSP**") is the Contractor providing the Cloud Service.

(h) "**Disaster Recovery Plan**" means a documented process or set of procedures to recover both the Cloud Service and UVic information in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures CSP is to follow in the event of a disaster.

(i) "**Incident Management Policy**" means the monitoring and detection of security events, and the execution of responses to those events.

(j) "**Information Incident**" is a suspected or known security incidents and information breaches or occurrences of unauthorized access to UVic's information.

(k) "**Infrastructure**" means infrastructure used by CSP or affiliates to provide or support the Cloud Service; components of this infrastructure may be physically located at UVic but administered by the CSP.

(l) "**Security Event Log**" means event logs that can be used in security, auditing or monitoring and can give rise to a security incident, information incident or security investigation. For clarity, Security Event Logs are not limited to those generated by security devices, but are those generated by all devices, systems and software that are technically capable of producing event logs that can be used in security investigations, auditing and monitoring. The guiding principle for Security Event Logs is the mandatory enablement of logging to ensure post determination of what identity performed what action, when, and from where (IP address).

(m) "**Security Incident Response Plan**" means an organized approach to addressing and managing the aftermath of a security breach or attack.

Purpose

2. The purpose of this Schedule is to:

(a) enable UVic to comply with its statutory obligations under the Act with respect to ensuring security arrangements for personal information; and

(b) ensure that, as a service provider, the Contractor is aware of and complies with its contractual requirements to handle information on behalf of the University of Victoria with appropriate security controls.

Security framework compliance and security controls attestation

3. The Contractor shall:

(a) ensure that the Cloud Service and Infrastructure used to manage the Cloud Service and Infrastructure and all data centers used in providing the Cloud Service and Infrastructure (including for management, back-up or disaster-recovery purposes) are compliant with one of the following international established cloud security frameworks: ISO 27017, NIST 800-53, CSA Cloud Controls Matrix (CCM);

(b) provide third party attestation of their security controls (e.g. SOC 2 Type 2 Compliance Report) to the University of Victoria annually for the duration of the service agreement; and
(c) ensure that any Cloud Service handling Payment Card Information (PCI) has the necessary Payment Card Industry Data Security Standards (PCI-DSS) compliance certifications in place and can provide these to the University of Victoria annually for the duration of the service agreement.

Enable security investigations through accurate logging

4. The Contractor shall:
(a) ensure Security Event Logs are logging all privileged and administrative account activity;
(b) ensure Security Event Logs include network flow information with sufficient detail to answer the question of how much data was exfiltrated and its destination IP address in the event of a security breach;
(c) retain online Security Event Log data for at least 90 days and provide access to the online system that holds this data to the University of Victoria;
(d) retain offline Security Event Log data for 1 year and provide to the University of Victoria upon request;
(e) ensure secure destruction of offline Security Event Log data older than 1 year and provide certificate of destruction to the University of Victoria upon request;
(f) protect the Security Event Logs and log generation systems from unauthorized access, modification, and deletion;
(g) protect the confidentiality and integrity of the centralized logs using encryption;
(h) transfer Security Event Logs regularly to a separate centralized logging system that is a physically different system or system component than the system producing the Security Event Logs, but with equivalent security safeguards, in order to ensure that logs are not lost due to component or system failure;
(i) ensure the Cloud Service offers the technical capability for UVic to enable or configure the forwarding/extraction/backup of Security Event Log data from the Cloud Service for forwarding/extraction/backup to UVic's Security Information and Event Management (SIEM) system;
(j) provide adequate support to UVic conducting its own security investigations into Information Incidents or compromises affecting UVic information;
(k) work with and support UVic if assistance is required in legal proceedings arising out of a breach; and
(l) implement, where supported by the available technology, the logical isolation of Security Event Logs related to UVic information and activities and ensure that logical isolation of Security Event Logs remains in effect at all times, even in the case of equipment or technology failure.

5. The Contractor shall, in accordance with industry best practices:
(a) ensure all Infrastructure devices and systems are synchronized with a Master Network Time Server that in turn are synchronized to authoritative Stratum 1 time servers; and
(b) time synchronization occurs at a minimum once per day.

Enable annual security threat and risk assessments

6. The Contractor shall:
(a) provide UVic with documentation, including architecture diagrams, service architecture, security controls architecture, technical information (that may be sanitized by the CSP to remove any proprietary or customer specific personal information) necessary for UVic to assess security threats and risks to how the data will be handled per its Information Security Data Classifications defined in the University of Victoria's Information Security Policy (IM7800);
(b) provide support to UVic to enable UVic to complete, and repeat annually, a security threat and risk assessment of the Cloud Service and assess the risk associated with the Cloud Service provided by the CSP; and
(c) provide UVic the required information and support via technical and security resources that can provide security and technical information regarding the CSP Infrastructure and Cloud Service implementation to enable UVic to assess risk.

Detect, investigate, and report Information Incidents

7. The Contractor shall:
(a) immediately notify UVic Information Security Office via email to infosec@uvic.ca of potential, suspected or known Information Incidents that may affect any of UVic's Information;
(b) take appropriate actions to remediate Information Incidents;
(c) implement continuous, real-time monitoring of the Security Event Logs for Information Incidents from the available sources using automated tools such as a SIEM system or equivalent;

(d) ensure that the CSP's incident response teams, tools and processes monitor the real-time alerts from the monitoring systems;
(e) implement privileged and administrative account activity monitoring and review by its incident response teams;
(f) conduct a security investigation in the case of Information Incidents discovered by or reported to CSP and provide UVic a copy of the investigation report. CSP to maintain chain of custody in their security investigations; and
(g) implement forensic and digital evidence practices and controls that conform or comply with industry best practices and relevant domain specific standards such as NIST 800-86 (Guide to Integrating Forensic Techniques into Incident Response), ISO 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence) or equivalent.

Hygiene-level security and process controls

Network:

8. The Contractor shall, in accordance with industry best practices:
(a) implement stateful packet inspection firewalls to control traffic flow to and from the CSP's systems, infrastructure, data center, Infrastructure and Cloud Service at all times, and configure the stateful packet inspection firewalls using industry best practices, and following the principles of least privilege;
(b) implement an Intrusion Prevention System (IPS) to control and filter traffic flow leaving and entering the CSP's systems, infrastructure, data center, Infrastructure and Cloud Service at all times, and configure the IPS using industry best practices;
(c) implement a secure perimeter, network segmentation, and ensure all network ingress/egress points are documented and strictly controlled; and
(d) ensure the Infrastructure has policy enforcement points (firewalls) controlling access between network zones that meet or exceed industry standards.

9. The Contactor shall, in accordance with industry best practices:
(a) ensure the management network for the Infrastructure will remain logically separated from any other network zone and it will not be directly accessible from the Internet;
(b) ensure the management network for the Infrastructure is internally segmented, with each server's dedicated network interface on its own segmented network;
(c) ensure interfaces on the management network do not have visibility to each other; and
(d) ensure all access to the management network is strictly controlled and exclusively enforced though the use of a secure access gateway or bastion host.

10. The contractor shall implement and maintain a distributed denial of service attack protection of the Cloud Service and the Infrastructure which meets or exceeds industry standards.

Databases:

11. The Contractor shall, in accordance with industry best practices:
(a) ensure that database maintenance utilities that bypass controls are restricted and monitored;
(b) unless prohibited by law, not permit third-party access without notifying UVic and giving UVic an opportunity to assess or contest the access request;
(c) implement methods to check and maintain the integrity of the data (e.g. consistency checks, checksums);
(d) implement encryption of UVic information stored in databases using whole database encryption (preferred) or table/column encryption where whole database encryption is not possible;
(e) implement logical isolation of all UVic information stored in databases using table/column logical isolation; and
(f) implement logical isolation of all UVic information stored in databases using a separate database instance dedicated to UVic information.

Workstations:

12. The Contractor shall, in accordance with industry best practices:
(a) ensure that all workstations used in the management and provision of the Cloud Service, and all workstations that are used to access the Infrastructure have appropriate industry best-practices security in place;
(b) ensure antivirus protection active at all times, and antivirus scans are configured for, at minimum, weekly; and
(c) ensure all such workstations will have all patches and appropriate security updates completed, at minimum, monthly for the operating system and all software installed on the workstation.

Servers:

13. The Contractor shall, in accordance with industry best practices:

(a) ensure the Cloud Service has antivirus and malware protection configured and active within the Cloud Service at all times;
(b) ensure antivirus and anti-malware definitions are updated daily;
(c) ensure antivirus and anti-malware protection are implemented on all relevant Infrastructure servers; and
(d) ensure all relevant Infrastructure servers are configured to undergo a full anti-virus and anti-malware scan for infections on at least a weekly basis.

14. The Contractor shall, in accordance with industry best practices:
(a) implement system and server hardening practices and controls for the Infrastructure that conform or comply with industry best practices and relevant domain specific standards such as NIST 800-123 (Guide to General Server Security) and CIS Benchmarks prior to placing the system into production;
(b) remove or disable all unsecured and unneeded ports, services, applications, accounts, protocols and network communicating applications on all systems and servers of the Infrastructure;
(c) use the principle of least privilege, when it configures and makes operational, only those ports, services, applications, protocols and applications necessary based on the functional requirements of the specific system or server of the Infrastructure;
(d) ensure default passwords are changed and shared accounts are not used; and
(e) ensure all passwords are longer than eight characters and include letters, numbers, and special characters.

15. The Contractor shall, in accordance with industry best practices:
(a) ensure that all Infrastructure has all available software patches installed on a regular schedule and ensure that the operating system and software versions are maintained at the most current available version (N) or one version earlier to the most current available version (N-1);
(b) ensure that all operating system and software vulnerabilities are remedied and patches installed on an accelerated/emergency basis for zero-day, critical and high risk vulnerabilities;
(c) implement appropriate mitigation measures promptly on notification of the zero-day vulnerability and mitigate critical and zero-day vulnerabilities immediately, or as soon as possible, and, in any event, within 24 hours;
(d) remediate all zero-day, high-risk and critical vulnerabilities through patching, decommissioning, or compensating controls;
(e) patch high-risk vulnerabilities within 15 days or less;
(f) patch medium-risk vulnerabilities within 90 days or less;
(g) document, follow, review, and update regularly a vulnerability management and patching policy; and
(h) review and update the current vulnerability management and patching policy annually.

Applications:

16. The Contractor shall, in accordance with industry best practices:
(a) ensure that a web application firewall - application layer (Layer 7) filtering will be implemented to protect web applications from, and mitigate the effect of, application attacks such as, without limitation, brute force, OWASP Top 10, OWASP Core rule set 3.0/2.2.9, SQL injection, cross-site scripting;
(b) ensure applications and programming interfaces are developed according to industry standards; and
(c) ensure it uses secure development practices for the ongoing development of the Cloud Service.

Physical Facilities:

17. The Contractor shall, in accordance with industry best practices:
(a) develop, document, disseminate and adhere to a physical and environmental protection policy for the facility in which the Infrastructure is located which meets or exceeds industry best practices;
(b) review and update the current physical and environmental protection policy annually;
(c) review and update the current physical and environmental protection procedures annually; and
(d) retain, maintain and review physical access logs at least monthly.

Change Control and Management:

18. The Contractor shall, in accordance with industry best practices:
(a) ensure change control processes for the Cloud Service are implemented and maintained in line with applicable industry best practices and standards to reduce security-related risks with respect to implemented changes;
(b) ensure adequate testing of any change for the Cloud Service is completed either before or during the implementation of such change but before being put into production;
(c) ensure the change control policy for the Cloud Service is documented, followed, reviewed, updated, and tested regularly; and

(d) ensure changes to the Cloud Service (not including data changes through the service) go through the change management process, including notification, testing, acceptance and implementation.

19. The Contractor shall, in accordance with industry best practices, perform security testing of all significant changes to the Infrastructure (such as operating system, database and applications) prior to placing changes into production as part of the change management process for the hosting environment.

20. The Contractor shall, in accordance with industry best practices:

(a) conduct vulnerability scans for published vulnerabilities in accordance with industry best practices for all Infrastructure components before rollout to production and after any major changes. The CSP must remedy any vulnerabilities identified by the scan before rolling into production the identified infrastructure components;

(b) implement vulnerability scans for all Infrastructure components when new vulnerabilities potentially affecting the systems and applications are identified and reported. The CSP shall remedy any vulnerabilities identified by the scan as appropriate ;and

c) scan for vulnerabilities all the Infrastructure components providing the services to which this schedule applies (including, but not limited to, servers, databases, applications, routers, firewalls, switches, and all associated infrastructure used to manage and monitor the services) on a regular basis, and in any event not less than once per month.

Security Threat & Risk Assessments:

21. The Contractor shall, in accordance with industry best practices:

(a) ensure that threat and risk assessments are undertaken for updates to Cloud Services or Infrastructure;

(b) ensure that threat and risk assessments are undertaken for new Cloud Services or Infrastructure;

(c) conduct security assessments regularly against an established security standard; and

(d) ensure threat and risk assessments are scheduled annually for existing Cloud Services or Infrastructure.

22. The Contractor shall, in accordance with industry best practices, conduct penetration tests of the Cloud Service and Infrastructure as part of its regular security assessments.

Information Security and Incident Response Policies:

23. The Contractor shall, in accordance with industry best practices:

(a) ensure its information security policy is documented, approved, followed, reviewed, and updated regularly;

(b) ensure its information security policy is based on and conforms to recognized industry standards;

(c) review and update the current information security policy at a minimum annually; and

(d) ensure it has documented and implemented an acceptable use policy which is based on and conforms to recognized industry standards.

24. The Contractor shall ensure that an Incident Response and Management policy which meets or exceeds industry best practices is documented, followed, reviewed, updated, and tested regularly.

Data Handling

25. The Contractor shall, in accordance with industry best practices:

(a) ensure development, test and training environments use clean test data; if sensitive production data is needed for these environments, the data shall be obfuscated (for example, using data masking functionality);

(b) provide the ability to perform obfuscation on data held in non-production environments; and

(c) ensure the development, test and training environments are separated from production environment and the separation is maintained at all times, even in the case of equipment or technology failure.

26. The Contractor shall, in accordance with industry best practices:

(a) ensure a Backup Policy which meets or exceeds industry best practices is documented, followed, reviewed, updated, and tested regularly;

(b) ensure daily backups are taken and verified regularly in accordance with Backup Policy;

(c) ensure backups must be stored in a separate physical location than the Infrastructure that stores the original data but must be within the same country as the original data; and

(d) ensure backup data that requires encryption is encrypted with AES with a minimum key length of 256 bits.

27. The Contractor shall, in accordance with industry best practice, implement and maintain the logical isolation of UVic's information from the information of other clients and ensure that such logical isolation remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

28. The Contractor shall:

(a) implement encryption of data at rest for all UVic information;

(b) ensure that encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure;

(c) implement encryption for the transmission of data and data in transit for all UVic information; and

(d) ensure that the encryption for the transmission of data is end-to-end and the payload containing UVic information is not decrypted anywhere on the transmission path, even on a temporary basis.

29. The Contractor shall not place any UVic information on portable media for transport outside the CSP data center without UVic's prior written approval. If UVic agrees in writing to have its information transported via portable media outside the CSP data center, all portable media must be encrypted as per UVic provided requirements.

Business Continuity Plan and Disaster Recovery Plan

30. The Contractor shall, in accordance with industry best practices:

(a) ensure Business Continuity Plan is documented, followed, reviewed, updated, and tested regularly; and

(b) ensure Disaster Recovery Plan is documented, followed, reviewed, updated, and tested regularly.

Asset Management and Disposal:

31. The Contractor shall, in accordance with industry best practices:

(a) ensure that all assets disposal related to the services, including any encryption keys used to encrypt UVic data, will be performed in a secure manner; and

(b) ensure disposal policy meets industry best practices and is documented, followed, reviewed, and updated regularly, and it includes both hardware and software and other critical business assets associated with the Cloud Service and Infrastructure.

Security Awareness:

32. The Contractor shall, in accordance with industry best practices:

(a) implement a Security Awareness Program and Course program that is documented, followed, reviewed, and updated regularly;

(b) ensure CSP personnel are required to undergo regular information security training;

(c) provide information security training that educates users on common threats and impacts to business such as not sharing credentials, not clicking on suspicious links and attachments, reporting security incidents, maintaining clean desk, locking inactive systems, and concealing valuables;

(d) ensure initial and annual Security Awareness Training includes security best practices, threat recognition, compliance and policy requirements, and reporting obligations;

(e) ensure follow-up security awareness training is presented to all personnel; and

(f) ensure each CSP employee person who will provide Cloud Services under the Agreement will complete, at the CSP's expense, complete a security awareness program or course prior to that person providing those services to UVic.

Access control and account management standards

33. The Contractor shall:

(a) request UVic's approval before CSP personnel can access UVic's data to perform support, maintenance or operational activities on Cloud Service Customer Information; and

(b) ensure its employees do not have standing or ongoing access rights to UVic data, and access to provide technical or customer support is only done after gaining approval from UVic

34. The Contractor shall:

(a) support UVic single sign-on technologies for authentication (e.g. integration with SAML 2.0 compliant identity provider);

(b) assign access to users based on role information provided by UVic;

(c) ensure that access is not granted until the method of access is formally approved by UVic;

(d) ensure that the access control policy clearly state the information access privileges for each defined role in the service;

(e) implement a monitoring process to oversee, manage and review user access rights and roles at regular intervals; and

(f) conduct access reviews and reviews accounts for compliance with account management requirements annually or upon request from UVic.

35. Where integration with UVic single sign-on technologies will not be used, the Contractor shall, in accordance with industry best practices:

(a) implement an access control policy and associated access control procedures which meets or exceeds industry standards;

(b) document, follow, review, and update regularly the access control policies and procedures; the policies should address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges, and inactivity timeouts;

(c) ensure that employees, contractors or vendors are provided only with the access they require to perform their function, and are authorized to use; ensure that access to information and system functions is granted based on "need to know" and job function; ensure that all access to information and system functions is be role-based and maintains principle of least privileged access;

(d) identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse (e.g. separation of duties);

(e) provide the capability to expeditiously disconnect or disable all remote access to the Cloud Service within 15 minutes on a verified request from UVic;

(f) enforce a limit of not more than three consecutive invalid logon attempts by a user during a 15 minute time period, and automatically lock accounts for 30 minutes if limit reached;

(g) limit the number of concurrent sessions to 3 sessions for privileged access and 2 sessions for non-privileged access; and

(h) trigger a session lock after 15 minutes of inactivity.

36. The Contractor shall, in accordance with industry best practices:

(a) ensure that privileged accounts are not created until formally approved by UVic;

(b) de-provision privileged account access within 24 hours upon request from UVic;

(c) disable all privileged account accesses after 90 days of inactivity;

(d) ensure that the privilege assignment process includes verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not granted until formally approved by UVic;

(e) ensure that the access control policy clearly states the information access privileges for each defined role in the organization;

(f) maintain a current and accurate inventory of privileged accounts and review it on a regular basis to identify inactive and unauthorised accounts; and

(g) implement a formal process to assign defined roles to users.

Encryption standards

37. The Contractor shall, for all HTTPS communications:

(a) use AES with a minimum key length of 256 bits;

(b) use TLS 1.2 or above;

(c) disable all versions of SSL and TLS 1.1 or less;

(d) use an X.509 certificate for performing server authentication;

(e) use RSA keys with a minimum key length of 2048 bits;

(f) disable RC4;

(g) use an Extended Validation (EV) Certificate for public-facing sites where available; and

(h) use perfect forward secrecy where available.

38. The Contractor shall:

(a) ensure that the Cloud Service offers the technical capability of cryptographic key management in order to allow UVic to have the technical capability to manage encryption keys for the Cloud Service; and

(b) not hold or have access to the encryption keys if they are managed by UVic and used to encrypt UVic information.

Information destruction and disposal

39. The Contractor must ensure that it destroys data from development, test, production, and backup environments, including any encryption keys used to encrypt UVic data, after verified successful transfer to UVic within 30 days of termination or conclusion of contractual obligations, or as directed by UVic in accordance with the contract specifications.

Notice of non-compliance

40. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify UVic of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

41. In addition to any other rights of termination which UVic may have under the Agreement or otherwise at law, UVic may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect including but not limited to failure to comply with section 7, above.

Interpretation

42. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

43. Any reference to the “Contractor” in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

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