**Definitions**

1. In this Schedule,
2. “**Act**” means the *Freedom of Information and Protection of Privacy Act* including any regulation made under it;
3. “**Agreement**” means the agreement between the Regulator and the Contractor to which this Schedule is attached;
4. “**Business Day**” means a day, other than a Saturday or Sunday, on which the provincial government offices are open for regular business in British Columbia;
5. “**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
6. “**Contractor**” means the person retained to perform the services under the Agreement;
7. “**personal information**” means recorded information about an identifiable individual, other than contact information, collected, created or accessible by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement;
8. “**public body**” means “public body” as defined in the Act;
9. “**service provider**” means a person retained under a contract to perform services for a public body;
10. “**Third Party Hosting Provider**” means a third party that provides a platform or hosting service through which the Contractor delivers the services under the Agreement and to whom personal information is not accessible and as such, for the purposes of this Schedule, is not considered a subcontractor;
11. “**third party request for disclosure**” means a subpoena, warrant, order, demand or request from an authority inside or outside of Canada for the unauthorized disclosure of personal information to which the Act applies; and
12. “**unauthorized disclosure of personal information**” means disclosure of, production of or the provision of access to personal information to which the Act applies, if that disclosure, production or access is not authorized by the Act.

**Purpose**

1. The purpose of this Schedule is to:
	1. enable the BC Energy Regulator to comply with the Regulator’s statutory obligations under the Act with respect to personal information; and
	2. ensure that, as a service provider, the Contractor is aware of and complies with the Contractor’s statutory obligations under the Act with respect to personal information.

**Acknowledgements**

1. The Contractor acknowledges and agrees that it will comply with the requirements and restrictions established by [Part 3](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#part3) of the [*Freedom of Information and Protection of Privacy Act*](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00) in respect of personal information unless the Agreement otherwise specifies

**Collection of Personal Information**

1. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that relates directly to and is necessary for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement.
2. The Contractor must collect personal information directly from the individual the information is about unless:

(a) the Regulator provides personal information to the Contractor;

(b) the Agreement otherwise specifies; or

(c) the Regulator otherwise directs in writing.

1. Where the Contractor collects personal information directly from the individual the information is about, the Contractor must tell that individual:
2. the purpose for collecting it;
3. the legal authority for collecting it; and
4. the contact information of the individual designated by the Regulator to answer questions about the Contractor’s collection of personal information.

**Accuracy of Personal Information**

1. Where personal information is collected by the Contractor directly from the individual the information is about, the Contractor must make every reasonable effort to ensure the accuracy and completeness of any such information to be used by the Contractor or the Regulator to make a decision that directly affects that individual.

**Requests for Access to Personal Information**

1. If the Contractor receives a request for access to information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access. If the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official’s name or title and contact information to the person making the request.

**Correction of Personal Information**

1. Where personal information is collected by the Contractor directly from the individual the information is about, the Contractor will comply with sections 12 to 15, inclusive, of this Schedule, as applicable.
2. Within 5 Business Days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
3. When issuing a written direction under section 12, the Regulator must advise the Contractor of the date the correction request was received by the Regulator in order that the Contractor may comply with section 14.
4. Within 5 Business Days of correcting or annotating any personal information under section 12, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was received by the Regulator, the Contractor disclosed the information being corrected or annotated.
5. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official’s name or title and contact information to the person making the request.

**Protection of Personal Information**

1. Without limiting any other provision of the Agreement, the Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including without limitation by ensuring that the integrity of the personal information is preserved. Without limiting the general nature of the foregoing sentence, the Contractor will ensure that all personal information is securely segregated from any information under the control of the Contractor or third parties to prevent unintended mixing of personal information with other information or access to personal information by unauthorized persons and to enable personal information to be identified and separated from the information of the Contractor or third parties.

**Storage of and Access to Personal Information**

1. The Contractor must comply with the requirements under the Act concerning storage of personal information outside of Canada, including, if required by the Regulator, by supporting the Regulator with completion of such assessments as may be required by law.
2. The Contractor will not change the location where it stores personal information without receiving prior authorization from the Regulator in writing.
3. The Contractor will not authorize or assist a Third Party Hosting Provider to access any personal information without the prior written approval of the Regulator.
4. Without limiting any other provision of the Agreement, the Contractor will implement and maintain an access log documenting all access to personal information, including a list of all persons that access any personal information. The Contractor will provide a copy of the access log to the Regulator upon request.

**Retention of Personal Information**

1. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

**Use of Personal Information**

1. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement. For clarity, unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not anonymize, aggregate or otherwise alter or modify personal information, including by converting personal information into non-personal information, or analyze personal information (whether by manual or automated means) for any purpose, including for the purpose of developing insights, conclusions or other information from personal information.

**Metadata**

1. Where the Contractor has or generates metadata as a result of services provided to the Regulator, where that metadata is personal information, the Contractor will:
2. not use it or disclose it to any other party except where the Agreement otherwise specifies; and
3. remove or destroy individual identifiers, if practicable.

**Disclosure of Personal Information**

1. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information to any person other than the Regulator if the disclosure is for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement.
2. If in relation to personal information, the Contractor:
3. receives a third-party request for disclosure;
4. receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a third-party request for disclosure; or
5. has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a third-party request for disclosure,

subject to section 26, the Contractor must immediately notify the Regulator.

1. If the Contractor receives a third-party request described in section 25(a) or (b), but is unable to notify the Regulator as required by section 25, the Contractor must instead:
2. use its best efforts to direct the party making the third-party request to the Regulator;
3. provide the Regulator with reasonable assistance to contest the third-party request; and
4. take reasonable steps to challenge the third-party request, including by presenting evidence with respect to:
5. the control of personal information by the Regulator as a public body under the Act;
6. the application of the Act to the Contractor as a service provider to the Regulator;
7. the conflict between the Act and the third-party request; and
8. the potential for the Contractor to be liable for an offence under the Act as a result of complying with the third-party request.

**Notice of Unauthorized Disclosure**

1. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information, the Contractor must immediately notify the Regulator.

**Compliance with the Act and Directions**

1. The Contractor must in relation to personal information comply with:
2. the requirements of the Act applicable to the Contractor as a service provider, including any regulation made under the Act and the terms of this Schedule; and
3. any direction given by the Regulator under this Schedule.
4. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.
5. The Contractor will provide the Regulator with such information as may be reasonably requested by the Regulator to assist the Regulator in confirming the Contractor’s compliance with this Schedule.

**Notice of Non-Compliance**

1. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply in any respect, with any provision in this Schedule, the Contractor must promptly notify the Regulator 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**

1. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator 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.

**Interpretation**

1. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
2. Any reference to “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 the requirements of the Act applicable to them.
3. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
4. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act, including any regulation made under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
5. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of the Agreement or the law of any jurisdiction outside Canada.

If a provision of the main body of this Agreement conflicts with a provision of this Schedule, then unless expressly stated otherwise within the Agreement, the provision of this Schedule will prevail to the extent of such conflict.

1. **Definitions in this Schedule,**
2. “Cloud Services” means services made available to users on demand via the Internet that are characterised by resource pooling, rapid elasticity and measured services with broad network access. Cloud Services include Software as a Service, Platform as a Service and Infrastructure as a Service, as such terms are understood pursuant to definitions provided by the National Institute of Standards and Technology (NIST).
3. “Industry Best Practice” means best practices commonly recognized in the IT industry from time to time and applicable to the protection and security of sensitive information of a nature similar to Protected Information against unauthorised access, disclosure or use, or any unauthorized attempts to access, disclose or use such information.
4. “Protected Information” means any and all of:
5. “personal information” as defined in the Freedom of Information and Protection of Privacy Act, British Columbia;
6. information and records of information the Contractor is required to treat as confidential under the Agreement; and
7. records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked by the BCER as “Protected Information” or the BCER otherwise instructs the Contractor that the record is “Protected Information” under the Agreement.
8. “BCER Information” means information of the BCER, including without limitation any Protected Information, 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 therefrom.
9. “Services” means the services provided by the Contractor to the BCER under the Agreement and includes, if applicable, any Cloud Services.
10. “Systems” means any systems, subsystems, equipment, devices, infrastructure, networks, hardware and software used in connection with the Services, including for managing, operating or providing the Services.
11. **Applicability**

For greater clarity, unless otherwise specified in the Agreement, the terms and conditions of this Schedule apply to the provision of all Services by the Contractor, its subcontractors and their respective personnel. Any reference to Contractor herein will include all subcontractors, Contractor personnel and subcontractor personnel, as applicable.

1. **Industry Best Practice**

The Contractor must have in place and maintain security controls to protect Protected Information that conform to commonly accepted industry norms that a prudent operator providing similar services would have implemented. Without limitation, the Contractor will perform its obligations under this Schedule in a manner that best conforms to Industry Best Practice.

1. **IT security standards and frameworks**

The Contractor must follow an IT security standard or framework and have a mature implementation of the requirements in the standard or framework. Examples of an IT security standard or framework are:

1. CIS Controls
2. NIST Cybersecurity Framework
3. ISO 27000 Series
4. **Access Control**

With respect to the access, by any Contractor personnel, to any part of the Contractor’s Systems that may contain BCER Information, the Contractor must:

1. implement access control policies and procedures that address onboarding, offboarding, transition between roles, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts;
2. identify and segregate conflicting duties and areas of responsibility, such as separation of duties;
3. maintain a current and accurate inventory of computer accounts;
4. review the inventory of computer accounts on a regular basis to identify dormant, fictitious or unused accounts;
5. enforce principles of “least privilege” and “need to know”;
6. review user access rights on a regular basis to identify excessive privileges;
7. enforce a limit of logon attempts and concurrent sessions.
8. **Authentication**

Where the Contractor manages user authentication controls for Contractor personnel, the Contractor must:

1. enforce minimum password complexity;
2. limit password reuse or use of known risky passwords;
3. require regular change of passwords at predetermined intervals, or require password changes upon detection of risky behaviour or possible breach; and
4. require multi-factor authentication for regular and privileged access.
5. **Security Awareness**
6. The Contractor must ensure that all persons employed or retained to perform the Services receive security awareness training, annually and supervision at a level and in substance that is appropriate to that person’s position and the Contractor’s obligations under this Schedule.
7. The Contractor must not permit any person the Contractor hires or uses to accessor obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under the Agreement.
8. **Security Audit Log Generation and Retention for Cloud Services**

The Contractor must:

1. generate and retain security audit logs that are sufficiently detailed to determine who did what and when for a period of 90 days online;
2. provide real time access to logs;
3. provide the technical capability to forward the logs to the BCER (API or Syslog); and
4. correlate, monitor, and alert on logs.
5. **Investigations Support and Security Investigations**

The Contractor must:

1. retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to the BCER for retention;
2. provide reasonable investigative support to the BCER;
3. maintain chain of custody for evidence;
4. support e-discovery; and
5. maintain legal holds to meet needs of investigations and judicial requests.
6. **Vulnerability Scan/Penetration Testing**

The Contractor must conduct regular:

* 1. vulnerability scans;
	2. web application scans; and
	3. penetration tests.

Attestation letter(s) showing completion of testing may be required.

1. **Technical Configuration**

The Contractor must:

1. logically isolate and encrypt BCER Information;
2. ensure workstations and servers used in management and provisioning of the Services are secured with:
	1. anti-malware protection;
	2. endpoint detection and response solution;
	3. software or hardware firewall;
	4. centralized access control; and
	5. centralized security information and event management;
3. **Patch Management and Vulnerability Avoidance**

Patch management and vulnerability avoidance is applicable to both Contractor Systems and Cloud Services provided to the BCER.

The Contractor must:

1. remedy vulnerabilities in a timely manner according to criticality;
2. patch all Systems and software regularly according to industry best practices;
3. have an information security policy based on recognized industry standards;
4. apply system hardening methods in securing Systems; and
5. use secure coding practices when developing applications and application programming interfaces.
6. **Business Continuity, Disaster Recovery, and Backup Plans**

The Contractor must:

1. have a business continuity plan and a disaster recovery plan;
2. conduct backups of critical data following at minimum the “3-2-1 backup strategy”; and
3. review and test business continuity, disaster recovery, and backup plans and procedures regularly.
4. **Incident Response and Management**

The Contractor must:

1. have an incident management plan and an incident response plan; and
2. review and test both incident management and incident response plans annually.
3. **Notifications of Breaches**

The Contractor must notify the BCER within 24 hours of the Contractor’s identification of a breach or incident that has affected, or may affect, BCER Information.

1. **Notifications of Changes**

The Contractor must notify the BCER of any changes to the Contractor’s security policies, procedures or agreements that may materially lower the security of BCER Information.

1. **Asset Management and Disposal**

The Contractor must

* 1. maintain an inventory of BCER Information assets;
	2. upon completion of contract or subscription, and upon request of BCER, the Contractor will dispose of all BCER Information including data residing in backups and allow BCER to download all BCER Information.

(b) use secure methods when disposing of BCER Information Assets, and

(c) maintain records of BCER Information asset disposals.

1. **Physical Security**

The Contractor must:

1. develop, document, and disseminate a physical and environmental protection policy;
2. regularly review and update its current physical and environmental protection policy and procedures; and
3. review physical access logs at least once monthly.
4. **Threat and Risk Assessments**

The Contractor must:

1. conduct threat and risk assessments on any part of the Contractor’s Systems that is new, or has been materially changed since the last threat and risk assessment was conducted; and
2. support the BCER in completing Security Threat and Risk Assessments.
3. **Security Screening**

The Contractor must:

1. screen all Contractor personnel prior to Contractor authorizing access to BCER or Contractor Systems;
2. conduct criminal record checks on all Contractor personnel who have access to any BCER or Contractor Systems;
3. make a reasonable determination of whether the individual constitutes an unreasonable security risk taking into consideration the duties of the individual, the type and sensitivity of information to which the individual may be exposed, and all applicable laws; and
4. require all Contractor personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law.
5. **Supply Chain**

The Contractor must ensure that its suppliers and subcontractors involved in the provision of Services meet or exceed the standards set forth in this Schedule.

1. **Encryption**

The Contractor must:

1. implement and maintain modern encryption of BCER Information while at rest and in transit;
2. if required, offer the BCER the technical capability of cryptographic key management to allow the BCER to manage encryption keys in relation to BCER Information at rest and in transit;
3. not hold or have access to encryption keys if such encryption keys are managed by the BCER to encrypt BCER information at rest or in transit; and
4. not provide encryption keys used to secure BCER Information to a third party or the ability to break such encryption.
5. **Isolation Controls and Logical Isolation of Data**

The Contractor must:

1. implement and maintain the logical isolation of BCER Information, even in the case of equipment or technology failure;
2. implement, where supported by available technology, the logical isolation of audit records related to BCER Information and activities, even in the case of equipment or technology failure; segregate tenancy traffic from management network traffic; and
3. not use Protected Information for test or development purposes without the written approval of the BCER.
4. **Technical Network Controls**

The Contractor must implement:

1. firewalls, web application firewalls, distributed denial of service, network threat detection and intrusion prevention systems to control traffic flow to and from the Contractor’s Systems;
2. network segmentation of Contractor Systems containing critical information or infrastructure management;
3. data loss prevention or detection; and
4. secure remote access to the Contractor’s Systems by Contractor personnel and contractors.
5. **Cloud Services Authentication and Authorization**

Where the Contractor is providing a Cloud Service, these provisions must be accommodated:

1. Single Sign-On integration with the BCER Microsoft Entra tenant;
2. “Break glass” account may be required for critical systems;
3. Role based access control where the BCER manages user role membership either within the Cloud Service or via security groups in the BCER Microsoft Entra tenant; and
4. Discreet user roles for BCER IT management and business roles as required.
5. **Use of BCER Systems**

Use of BCER Systems by the Contractor or its personnel (including subcontractors) must be restricted to activities necessary for provision of the Services. The BCER reserves the right to not make any particular BCER facility, system, network or device available to the Contractor unless the Contractor or its individual personnel (as applicable) agree to any additional terms and conditions acceptable to the BCER.

1. **Security Contact**

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