Security Overview

Web Hosting Canada

Strike Graph

Prepared on Oct 01 2025

Company Overview

Web Hosting Canada (WHC) is a privately owned, Canadian technology and IT infrastructure company based in Montreal, Quebec. We're a team of passionate web professionals who's core mission is to help Canadians succeed online.
Since 2003, WHC has set the highest standard for service reliability and security and is now trusted by over 60,000 clients throughout Canada and abroad. It is among the fastest-growing web service providers in Canada. WHC is an ICANN and CIRA-accredited domain name registrar.

Risk Posture & Security Controls

To mitigate cyber security and information security risks, Web Hosting Canada has established the following security posture which is composed of security controls unique to Web Hosting Canada's environment. This posture is aligned to common risk categories for ease of use.

Access

The following controls mitigate risks related to logical access, including concepts like authentication and the appropriateness of access to information and data.

Mitigated and monitored by 13 control(s)

Separation of Duties: Developers

Access to the source code repository is restricted to authorized employees.

Covered Security Criteria: SOC2:2017.CC.6.3.3, SOC2:2017.CC.5.1.6, SOC2:2022.CC.8.1, SOC2:2022.CC.5.1,

Administrator Access

Administrator access to the application, database, VPN, and operating system is restricted to authorized users.

Covered Security Criteria: SOC2:2017.CC.6.2.1, SOC2:2017.CC.6.3.1, SOC2:2022.CC.6.3, SOC2:2022.CC.6.2,

Provisioning

Logical/physical user access requests are documented and require approval prior to access being provisioned.

Covered Security Criteria: SOC2:2017.CC.6.1.2, SOC2:2022.CC.6.4, SOC2:2022.CC.6.3, SOC2:2022.CC.6.2, SOC2:2022.CC.6.1,

Termination of Access

A user's physical and logical access to IT systems is revoked within 48 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.

Covered Security Criteria: SOC2:2017.CC.9.2.8, SOC2:2017.CC.6.3.2, SOC2:2017.CC.6.4.2, SOC2:2017.CC.6.2.2, SOC2:2022.CC.6.4, SOC2:2022.CC.6.3, SOC2:2022.CC.6.2,

User Authentication

Unique usernames and passwords are required to authenticate all users. Users are required to use non-privileged accounts or roles when accessing nonsecurity functions. Exceptions are approved by the Head of DevOps.

Covered Security Criteria: SOC2:2017.CC.6.1.3, SOC2:2017.CC.6.1.7, SOC2:2022.CC.6.1,

User Access Review

Management performs at least an annual review of user access to systems based on job duties. Inactive users are removed and removal is documented. The review is formally documented including system generated user listings and sign off by management.

Covered Security Criteria: SOC2:2017.CC.6.2.1, SOC2:2017.CC.6.2.2, SOC2:2017.CC.6.3.4, SOC2:2017.CC.5.2.3, SOC2:2017.CC.6.2.3, SOC2:2022.CC.5.2, SOC2:2022.CC.6.3, SOC2:2022.CC.6.2,

Logical Access

Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, secure authentication requirements, role-based access, and the principle of least privilege. The policy is reviewed annually.

Covered Security Criteria: SOC2:2017.CC.6.1.3, SOC2:2017.CC.6.1.5, SOC2:2017.CC.5.3.1, SOC2:2017.CC.6.1.2, SOC2:2017.CC.5.2.3, SOC2:2017.CC.6.3.1, SOC2:2022.CC.5.2,

Encryption at Rest

All data at rest is encrypted using industry standard algorithms.

Covered Security Criteria: SOC2:2017.CC.6.1.9, SOC2:2017.PI.1.5.1, SOC2:2022.PI.1.5, SOC2:2022.CC.6.1,

Encrypted Server Access

Production system access is encrypted to ensure communications with servers are secured. Devices accessing or connecting to the system are authenticated prior to access being granted.

Covered Security Criteria: SOC2:2017.CC.6.6.1, SOC2:2022.CC.6.6,

Encryption in Transit

Any sensitive data that is transmitted over public networks, and data in transit is encrypted.

Covered Security Criteria: SOC2:2017.CC.6.1.9, SOC2:2017.CC.6.7.2, SOC2:2017.PI.1.4.1, SOC2:2022.CC.6.7, SOC2:2022.PI.1.4, SOC2:2022.CC.6.1,

Vulnerability Scan

Vulnerability scans are performed quarterly to help identify security risks. Results are assessed and, where required, remediated.

Covered Security Criteria: SOC2:2017.CC.7.2.4, SOC2:2017.CC.7.1.4, SOC2:2017.CC.6.1.5, SOC2:2017.CC.7.2.2, SOC2:2017.CC.7.1.2, SOC2:2017.CC.6.8.2, SOC2:2017.CC.7.1.5, SOC2:2017.CC.5.3.4, SOC2:2017.CC.4.1.1, SOC2:2022.CC.7.2, SOC2:2022.CC.6.8, SOC2:2022.CC.4.1, SOC2:2022.CC.7.1, SOC2:2022.CC.5.3,

Firewall Rules

Firewall rulesets are configured and in place to help prevent unauthorized access threats from outside the application and infrastructure environment.

Covered Security Criteria: SOC2:2017.CC.6.6.1, SOC2:2022.CC.6.6,

Password Requirements

Authentication for the network, operating systems, databases, applications, cloud, and VPNs adheres to the company password setting requirements. These requirements are documented within the Logical Access Policy.

Covered Security Criteria: SOC2:2017.CC.6.2.1, SOC2:2022.CC.6.2,

Fraud

The following controls mitigate risks related to fraud, specifically as it relates to the legal concept of inappropriate action that leads to financial or personal gain.

Legal

The following controls mitigate risks related to the application (or lack of application) of laws, regulations, and contractual requirements applicable to Web Hosting Canada.

Mitigated and monitored by 5 control(s)

Contracts

The organization utilizes a standard contractual agreement that defines relevant security (and privacy) commitments and requirements for both its customers as well as third party providers; scope, responsibilities, compliance requirements, and service levels are included in the contract. The agreement template is periodically reviewed to align with business requirements.

> **Covered Security Criteria:** SOC2:2017.P.6.1.3, SOC2:2017.CC.2.3.10, SOC2:2017.P.6.4.1, SOC2:2017.CC.9.2.11, SOC2:2017.CC.2.3.6, SOC2:2017.CC.2.3.9, SOC2:2017.CC.2.2.10, SOC2:2017.CC.9.2.8, SOC2:2017.CC.9.2.1, SOC2:2017.CC.9.2.9, SOC2:2017.CC.9.2.4, SOC2:2017.CC.9.2.3, SOC2:2017.CC.2.3.8, SOC2:2017.CC.9.2.7, SOC2:2022.CC.2.3, SOC2:2022.P.6.4, SOC2:2022.CC.9.2, SOC2:2022.P.6.1,

Non Disclosure Agreement

Employees and contractors are required to sign a non-disclosure agreement upon hire. The non-disclosure agreement includes the signee's and the company's responsibility with respect to information security.

> **Covered Security Criteria:** SOC2:2017.CC.9.2.9, SOC2:2022.CC.1.4,

Data Retention/Deletion

Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.

> **Covered Security Criteria:** SOC2:2017.P.4.2.1, SOC2:2017.P.4.3.1, SOC2:2017.C.1.2.2, SOC2:2017.CC.6.5.2, SOC2:2017.C.1.2.1, SOC2:2017.C.1.1.2, SOC2:2022.P.3.2, SOC2:2022.C.1.2, SOC2:2022.P.4.2, SOC2:2022.C.1.1, SOC2:2022.P.4.3, SOC2:2022.CC.6.5,

Tech Competence

The new hire screening process includes a consideration of the skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Background/reference checks are required prior to hire.

> **Covered Security Criteria:** SOC2:2017.CC.1.4.1, SOC2:2017.CC.1.4.6, SOC2:2017.CC.1.4.5, SOC2:2017.CC.4.1.4, SOC2:2022.CC.4.1, SOC2:2022.CC.5.3, SOC2:2022.CC.1.4,

Risk Assessment Methodology

A risk assessment is conducted annually or in the event of significant changes to the organization and/or information systems. The risk assessment will identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.

> **Covered Security Criteria:** SOC2:2017.CC.3.3.1, SOC2:2017.CC.3.1.15, SOC2:2017.CC.3.3.3, SOC2:2017.CC.9.2.2, SOC2:2017.CC.3.2.6, SOC2:2017.CC.3.2.1, SOC2:2017.CC.3.2.4, SOC2:2017.CC.3.1.11, SOC2:2017.CC.3.3.5, SOC2:2017.CC.3.4.1, SOC2:2017.CC.3.4.4, SOC2:2017.CC.3.2.8, SOC2:2017.CC.5.1.3, SOC2:2017.CC.3.3.4, SOC2:2017.CC.3.2.3, SOC2:2017.CC.3.2.7, SOC2:2017.CC.2.1.1, SOC2:2017.CC.3.2.2, SOC2:2017.CC.9.2.3, SOC2:2017.CC.3.3.2, SOC2:2017.CC.3.4.2, SOC2:2017.CC.3.1.2, SOC2:2017.CC.3.4.5, SOC2:2022.CC.3.2, SOC2:2022.CC.5.1, SOC2:2022.CC.9.2, SOC2:2022.CC.3.4, SOC2:2022.CC.3.3, SOC2:2022.CC.3.1, SOC2:2022.CC.2.1, SOC2:2022.CC.9.1,

People

The following controls mitigate risks related to Web Hosting Canada's employees and other staff. Examples include dissatisfaction, attrition, and HR related events.

Mitigated and monitored by 12 control(s)

Employee Performance

A performance evaluation process is in place and employees are evaluated at least annually.

> **Covered Security Criteria:** SOC2:2017.CC.1.5.4, SOC2:2017.CC.1.4.2, SOC2:2017.CC.1.5.5, SOC2:2017.CC.1.1.3, SOC2:2017.CC.1.5.2, SOC2:2017.CC.1.5.3, SOC2:2017.CC.1.1.4, SOC2:2017.CC.1.5.1, SOC2:2022.CC.1.5, SOC2:2022.CC.1.1, SOC2:2022.CC.1.4,

Tech Competence

The new hire screening process includes a consideration of the skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Background/reference checks are required prior to hire.

> **Covered Security Criteria:** SOC2:2017.CC.1.4.1, SOC2:2017.CC.1.4.6, SOC2:2017.CC.1.4.5, SOC2:2017.CC.4.1.4, SOC2:2022.CC.4.1, SOC2:2022.CC.5.3, SOC2:2022.CC.1.4,

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

> **Covered Security Criteria:** SOC2:2017.CC.2.2.3, SOC2:2017.CC.7.4.1, SOC2:2017.P.8.1.5, SOC2:2017.CC.2.2.6, SOC2:2017.P.8.1.4, SOC2:2017.CC.9.2.4, SOC2:2017.CC.7.3.2, SOC2:2017.P.6.5.1, SOC2:2017.CC.2.3.5, SOC2:2017.CC.7.3.4, SOC2:2017.P.6.3.1, SOC2:2022.P.8.1, SOC2:2022.CC.7.3, SOC2:2022.CC.7.4, SOC2:2022.CC.2.2, SOC2:2022.CC.9.2, SOC2:2022.P.6.3,

Security Training

Employees complete security-related training, as relevant to their duties, upon hire and on an annual basis. The annual security training includes information on how to report security incidents and concerns.

> **Covered Security Criteria:** SOC2:2017.CC.2.2.1, SOC2:2017.CC.5.3.1, SOC2:2017.CC.2.2.6, SOC2:2017.CC.2.2.8, SOC2:2017.CC.2.2.5, SOC2:2017.CC.1.5.1, SOC2:2022.CC.2.2,

Employee Shared Drive

A centralized drive is in place for employees to access all corporate policies and procedures as well as job descriptions.

> **Covered Security Criteria:** SOC2:2017.CC.2.2.1, SOC2:2022.CC.2.2,

Management Oversight

Company founders and department leads meet at least quarterly to assess organizational objectives.

> **Covered Security Criteria:** SOC2:2022.CC.1.2,

Organizational Chart

The business is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned. Organizational charts are updated as needed.

> **Covered Security Criteria:** SOC2:2017.CC.1.3.2, SOC2:2017.CC.1.3.3, SOC2:2022.CC.1.3,

Job Descriptions

Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.

Covered Security Criteria: SOC2:2017.CC.1.4.1, SOC2:2017.CC.1.4.3, SOC2:2017.CC.5.3.5, SOC2:2017.CC.2.2.1, SOC2:2017.CC.2.2.9, SOC2:2017.CC.1.3.3, SOC2:2022.CC.2.2, SOC2:2022.CC.1.4, SOC2:2022.CC.1.3,

Information Security Policy

The Information Security Policy is maintained, reviewed, and updated annually by management.

Covered Security Criteria: SOC2:2017.CC.2.2.10, SOC2:2022.CC.5.3,

Internal Controls

Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review. Controls are reasssed each year to determine relevance to the control environment.

Covered Security Criteria: SOC2:2017.CC.2.3.10, SOC2:2017.CC.5.3.2, SOC2:2017.CC.5.3.5, SOC2:2017.P.8.1.6, SOC2:2017.CC.5.1.5, SOC2:2017.CC.5.1.2, SOC2:2017.CC.5.3.3, SOC2:2017.CC.2.2.1, SOC2:2017.CC.4.1.3, SOC2:2017.CC.2.2.5, SOC2:2017.CC.1.5.1, SOC2:2022.P.8.1, SOC2:2022.CC.1.5, SOC2:2022.CC.4.2, SOC2:2022.CC.5.1, SOC2:2022.CC.4.1, SOC2:2022.CC.2.2, SOC2:2022.CC.5.3,

Employee Acceptable Use Policy

An Acceptable Use Policy is documented, which outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services.

Covered Security Criteria: SOC2:2017.CC.2.2.9, SOC2:2022.CC.2.2,

Organizational Evaluation

The Executive Leadership Team and the Board of Directors evaluate the organizational structure, reporting lines, authorities, and roles on at least annually to help support the achievement of business objectives.

Covered Security Criteria: SOC2:2017.CC.1.2.2, SOC2:2017.CC.5.3.2, SOC2:2017.CC.1.2.4, SOC2:2017.CC.1.1.1, SOC2:2017.CC.1.3.2, SOC2:2017.CC.1.2.1, SOC2:2017.CC.1.3.5, SOC2:2017.CC.2.2.2, SOC2:2017.CC.1.3.3, SOC2:2022.CC.1.3, SOC2:2022.CC.1.2,

Physical

The following controls mitigate risks related to physical access, such as doors, loading docks, copy rooms, server rooms. This also includes any environmental risks, such as fires, floods, or earthquakes.

Mitigated and monitored by 1 control(s)

Termination of Access

A user's physical and logical access to IT systems is revoked within 48 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.

Covered Security Criteria: SOC2:2017.CC.9.2.8, SOC2:2017.CC.6.3.2, SOC2:2017.CC.6.4.2, SOC2:2017.CC.6.2.2, SOC2:2022.CC.6.4, SOC2:2022.CC.6.3, SOC2:2022.CC.6.2,

Policy

The following controls mitigate risks related to how information security is governed at Web Hosting Canada. This includes policy, procedures, work instructions, and how they are communicated throughout the organization.

Mitigated and monitored by 13 control(s)

Data Flow Diagram

The data flow diagram is maintained and highlights the systems that require logical access controls per data classification level. The data flow diagram is updated annually or as business needs require.

> **Covered Security Criteria:** SOC2:2017.CC.3.2.6, SOC2:2017.CC.6.1.5, SOC2:2017.CC.5.1.3, SOC2:2017.CC.2.2.9, SOC2:2017.PI.1.1.2, SOC2:2022.CC.2.1, SOC2:2022.CC.2.2, SOC2:2022.CC.6.1,

Asset Inventory

An inventory of information assets, including hardware, software, is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.

> **Covered Security Criteria:** SOC2:2017.CC.3.2.6, SOC2:2017.C.1.1.1, SOC2:2017.CC.6.1.1, SOC2:2017.PI.1.1.2, SOC2:2022.CC.2.1, SOC2:2022.C.1.1, SOC2:2022.CC.6.1,

Data Retention/Deletion

Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.

> **Covered Security Criteria:** SOC2:2017.P.4.2.1, SOC2:2017.P.4.3.1, SOC2:2017.C.1.2.2, SOC2:2017.CC.6.5.2, SOC2:2017.C.1.2.1, SOC2:2017.C.1.1.2, SOC2:2022.P.3.2, SOC2:2022.C.1.2, SOC2:2022.P.4.2, SOC2:2022.C.1.1, SOC2:2022.P.4.3, SOC2:2022.CC.6.5,

Data Management Policy

A defined Data Management Policy provides guidance on information categories, usage, storage, and transmission of data. This policy is reviewed, updated, and approved annually.

> **Covered Security Criteria:** SOC2:2017.C.1.1.1, SOC2:2017.P.4.2.2, SOC2:2017.P.4.3.1, SOC2:2017.C.1.2.2, SOC2:2017.CC.6.5.2, SOC2:2017.C.1.2.1, SOC2:2022.C.1.2, SOC2:2022.P.4.2, SOC2:2022.C.1.1, SOC2:2022.P.4.3, SOC2:2022.CC.6.5,

Data Classification Policy

A defined information classification scheme has been established to label and handle data. This policy is reviewed, updated, and approved annually. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, sensitive.

> **Covered Security Criteria:** SOC2:2017.CC.6.1.6, SOC2:2017.CC.3.2.6, SOC2:2017.C.1.1.1, SOC2:2017.A.1.2.7, SOC2:2017.PI.1.1.2, SOC2:2022.CC.2.1, SOC2:2022.C.1.1, SOC2:2022.CC.6.1, SOC2:2022.A.1.2,

Disaster Recovery & Business Continuity

A Disaster Recovery & Business Continuity Plan has been developed. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality in the event of major disruption. The plan is reviewed and tested annually. Disaster recovery is included within the Business Continuity Plan.

> **Covered Security Criteria:** SOC2:2017.CC.3.2.1, SOC2:2017.A.1.2.3, SOC2:2017.A.1.3.1, SOC2:2017.CC.9.1.1, SOC2:2017.CC.5.1.2, SOC2:2017.A.1.2.10, SOC2:2017.CC.5.2.1, SOC2:2022.CC.5.1, SOC2:2022.CC.9.1,

Restore

Documented backup and restoration procedures for the network are maintained and reviewed annually. Backup restoration testing is performed at least annually.

> **Covered Security Criteria:** SOC2:2017.CC.7.5.1, SOC2:2017.A.1.3.2, SOC2:2022.CC.7.5, SOC2:2022.CC.7.4, SOC2:2022.A.1.3,

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

> **Covered Security Criteria:** SOC2:2017.CC.2.2.3, SOC2:2017.CC.7.4.1, SOC2:2017.P.8.1.5, SOC2:2017.CC.2.2.6, SOC2:2017.P.8.1.4, SOC2:2017.CC.9.2.4, SOC2:2017.CC.7.3.2, SOC2:2017.P.6.5.1, SOC2:2017.CC.2.3.5, SOC2:2017.CC.7.3.4, SOC2:2017.P.6.3.1, SOC2:2022.P.8.1, SOC2:2022.CC.7.3, SOC2:2022.CC.7.4, SOC2:2022.CC.2.2, SOC2:2022.CC.9.2, SOC2:2022.P.6.3,

Incident Response: Process

The incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security, confidentiality, or privacy.

> **Covered Security Criteria:** SOC2:2017.CC.7.5.1, SOC2:2017.CC.7.4.2, SOC2:2017.CC.7.4.6, SOC2:2017.CC.7.3.3, SOC2:2017.CC.7.4.7, SOC2:2017.CC.7.4.5, SOC2:2017.CC.7.4.3, SOC2:2017.CC.7.3.2, SOC2:2017.CC.7.5.5, SOC2:2017.CC.7.5.2, SOC2:2017.CC.7.4.4, SOC2:2017.CC.7.3.4, SOC2:2017.CC.7.5.3, SOC2:2017.CC.7.4.11, SOC2:2017.CC.7.3.1, SOC2:2022.CC.7.3, SOC2:2022.CC.2.3, SOC2:2022.CC.7.5, SOC2:2022.CC.7.4,

Incident Response: Testing

The security incident response plan is tested on at least an annual basis.

> **Covered Security Criteria:** SOC2:2017.CC.7.4.1, SOC2:2017.CC.2.2.6, SOC2:2017.CC.7.4.10, SOC2:2022.CC.7.5, SOC2:2022.CC.7.4,

Incidents External

External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organization's support webpage. The incident is documented in accordance with the Incident Response Plan, if required.

> **Covered Security Criteria:** SOC2:2017.P.6.5.2, SOC2:2017.CC.2.2.3, SOC2:2017.CC.2.3.2, SOC2:2017.CC.9.2.4, SOC2:2017.CC.2.3.4, SOC2:2017.CC.2.3.11, SOC2:2022.CC.2.3, SOC2:2022.CC.9.2, SOC2:2022.CC.2.2, SOC2:2022.P.6.5,

Information Security Policy

The Information Security Policy is maintained, reviewed, and updated annually by management.

> **Covered Security Criteria:** SOC2:2017.CC.2.2.10, SOC2:2022.CC.5.3,

Internal Controls

Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review. Controls are reasssed each year to determine relevance to the control environment.

> **Covered Security Criteria:** SOC2:2017.CC.2.3.10, SOC2:2017.CC.5.3.2, SOC2:2017.CC.5.3.5, SOC2:2017.P.8.1.6, SOC2:2017.CC.5.1.5, SOC2:2017.CC.5.1.2, SOC2:2017.CC.5.3.3, SOC2:2017.CC.2.2.1, SOC2:2017.CC.4.1.3, SOC2:2017.CC.2.2.5, SOC2:2017.CC.1.5.1, SOC2:2022.P.8.1, SOC2:2022.CC.1.5, SOC2:2022.CC.4.2, SOC2:2022.CC.5.1, SOC2:2022.CC.4.1, SOC2:2022.CC.2.2, SOC2:2022.CC.5.3,

Privacy

The following controls mitigate risks related to any of Web Hosting Canada’s operations that can be tied to or attributed to the personal or protected data of an individual.

Mitigated and monitored by 2 control(s)

Incident Response: Employee Responsibility

A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.

Covered Security Criteria: SOC2:2017.CC.2.2.3, SOC2:2017.CC.7.4.1, SOC2:2017.P.8.1.5, SOC2:2017.CC.2.2.6, SOC2:2017.P.8.1.4, SOC2:2017.CC.9.2.4, SOC2:2017.CC.7.3.2, SOC2:2017.P.6.5.1, SOC2:2017.CC.2.3.5, SOC2:2017.CC.7.3.4, SOC2:2017.P.6.3.1, SOC2:2022.P.8.1, SOC2:2022.CC.7.3, SOC2:2022.CC.7.4, SOC2:2022.CC.2.2, SOC2:2022.CC.9.2, SOC2:2022.P.6.3,

Incidents External

External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organization's support webpage. The incident is documented in accordance with the Incident Response Plan, if required.

Covered Security Criteria: SOC2:2017.P.6.5.2, SOC2:2017.CC.2.2.3, SOC2:2017.CC.2.3.2, SOC2:2017.CC.9.2.4, SOC2:2017.CC.2.3.4, SOC2:2017.CC.2.3.11, SOC2:2022.CC.2.3, SOC2:2022.CC.9.2, SOC2:2022.CC.2.2, SOC2:2022.P.6.5,

Software

The following controls mitigate risks related to the use of protection of any applications or code, whether proprietary or provided by others.

Technical

The following controls mitigate risks related to anything having to do with how the network operates. This includes firewalls, data loss prevention, and network operations.

Mitigated and monitored by 15 control(s)

Change Management: Segregation of Duties

Segregation of duties exist during the infrastructure and application change process.

Covered Security Criteria: SOC2:2017.CC.6.3.3, SOC2:2017.CC.5.1.6, SOC2:2022.CC.5.1,

Change Management: Ticketing System

A centralized ticketing and workflow tool tracks software change activity, including development and testing.

Another tool tracks approvals.

Covered Security Criteria: SOC2:2017.CC.8.1.4, SOC2:2017.CC.8.1.9, SOC2:2017.CC.8.1.8, SOC2:2022.CC.8.1,

Change Management: Emergency Process

An emergency change process is followed for changes required in urgent situations.

Covered Security Criteria: SOC2:2017.CC.8.1.13, SOC2:2022.CC.8.1,

Change Management Policy

A Change Management Policy and Procedures are in place to request, document, test, and approve changes. The Head of DevOps is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on operations. All technology acquisition, development, and maintenance processes are governed by change management procedures. The policy is reviewed at

least annually and re-distributed to staff, as needed.

Covered Security Criteria: SOC2:2017.CC.6.8.3, SOC2:2017.CC.5.2.4, SOC2:2017.CC.8.1.3, SOC2:2017.CC.8.1.1, SOC2:2017.CC.8.1.2, SOC2:2022.CC.8.1, SOC2:2022.CC.5.2, SOC2:2022.CC.6.8, SOC2:2022.CC.6.1,

Change Management: Application/Software

All application changes for internally developed software are developed, tested, and approved prior to implementation.

Covered Security Criteria: SOC2:2017.CC.8.1.2, SOC2:2022.CC.8.1,

Change Management: Infrastructure

Infrastructure changes are tested, reviewed, and approved by authorized personnel prior to implementation.

Covered Security Criteria: SOC2:2017.CC.8.1.10, SOC2:2017.CC.8.1.7, SOC2:2022.CC.8.1, SOC2:2022.A.1.1,

Antivirus

Antivirus is installed on all workstations and servers to help protect against viruses and malicious software on the systems.

Covered Security Criteria: SOC2:2017.CC.6.8.4, SOC2:2022.CC.6.7, SOC2:2022.CC.6.8,

Disk Encryption

Disk encryption is setup and verified on all employee devices.

Covered Security Criteria: SOC2:2017.CC.6.1.9, SOC2:2017.CC.6.7.2, SOC2:2022.CC.6.1,

Vulnerability Scan

Vulnerability scans are performed quarterly to help identify security risks. Results are assessed and, where required, remediated.

Covered Security Criteria: SOC2:2017.CC.7.2.4, SOC2:2017.CC.7.1.4, SOC2:2017.CC.6.1.5, SOC2:2017.CC.7.2.2, SOC2:2017.CC.7.1.2, SOC2:2017.CC.6.8.2, SOC2:2017.CC.7.1.5, SOC2:2017.CC.5.3.4, SOC2:2017.CC.4.1.1, SOC2:2022.CC.7.2, SOC2:2022.CC.6.8, SOC2:2022.CC.4.1, SOC2:2022.CC.7.1, SOC2:2022.CC.5.3,

Penetration Test

An independent, third party provider is contracted to perform penetration tests at least annually, or as business needs require. Test results are reviewed and tracked to resolution.

Covered Security Criteria: SOC2:2017.CC.7.2.4, SOC2:2017.CC.4.1.6, SOC2:2017.CC.4.1.8, SOC2:2017.CC.2.3.3, SOC2:2017.CC.4.2.1, SOC2:2017.CC.4.1.5, SOC2:2017.CC.5.3.4, SOC2:2017.CC.4.1.1, SOC2:2022.CC.4.1, SOC2:2022.CC.4.2, SOC2:2022.CC.5.3,

Network Diagram

System boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.

Covered Security Criteria: SOC2:2017.CC.3.2.6, SOC2:2017.CC.5.1.3, SOC2:2017.CC.2.2.9, SOC2:2022.CC.2.1, SOC2:2022.CC.2.2,

Configuration Standards

A baseline security configuration is maintained by the information technology team and is deployed to all systems; the baseline settings are reviewed annually or as business needs change.

Covered Security Criteria: SOC2:2017.CC.7.1.1, SOC2:2017.CC.8.1.12, SOC2:2022.CC.8.1, SOC2:2022.CC.7.1,

Intrusion Detection

Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.

> **Covered Security Criteria:** SOC2:2017.CC.7.2.3, SOC2:2017.CC.6.6.4, SOC2:2017.CC.7.2.2, SOC2:2017.CC.7.1.2, SOC2:2017.CC.5.3.4, SOC2:2017.CC.4.1.1, SOC2:2017.CC.7.2.1, SOC2:2022.CC.7.2, SOC2:2022.CC.4.1, SOC2:2022.CC.6.6, SOC2:2022.CC.7.1,

Monitoring Infrastructure

IT infrastructure monitoring tools are configured to monitor IT infrastructure availability and performance, generate alerts when specific predefined thresholds are met or exceeded, and forecast capacity requirements to ensure system performance. Threat intelligence feeds are utilized.

> **Covered Security Criteria:** SOC2:2017.A.1.2.5, SOC2:2017.A.1.2.6, SOC2:2017.A.1.1.3, SOC2:2017.A.1.2.3, SOC2:2017.A.1.2.4, SOC2:2017.A.1.1.2, SOC2:2017.A.1.1.1, SOC2:2017.A.1.2.2, SOC2:2017.CC.4.1.3, SOC2:2022.CC.4.1, SOC2:2022.A.1.1,

Separation of Environments

Production and development environments are logically and physically separated.

> **Covered Security Criteria:** SOC2:2017.CC.8.1.15, SOC2:2022.CC.8.1,

Vendor

The following controls mitigate risks related to any supplier or service provider, including contractors, consultants, and cloud providers.

Mitigated and monitored by 5 control(s)

Vendor Due Diligence

Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.

> **Covered Security Criteria:** SOC2:2017.CC.1.1.5, SOC2:2017.CC.9.2.1, SOC2:2017.CC.1.4.6, SOC2:2022.P.6.4, SOC2:2022.CC.9.2, SOC2:2022.CC.3.4,

Third Party SOC2

Critical vendors' SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.

> **Covered Security Criteria:** SOC2:2017.CC.9.2.2, SOC2:2017.CC.9.2.6, SOC2:2017.CC.3.2.1, SOC2:2017.CC.9.2.12, SOC2:2017.CC.9.2.10, SOC2:2017.CC.3.1.9, SOC2:2017.CC.3.4.5, SOC2:2022.CC.9.2,

Vendor Management Policy

A policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.

> **Covered Security Criteria:** SOC2:2017.CC.9.2.5, SOC2:2017.CC.9.2.1, SOC2:2022.CC.3.2, SOC2:2022.P.6.4, SOC2:2022.CC.9.2,

Vendor Risk Register

A register of all vendors and service providers is maintained. The register includes vendor risk level which is assessed prior to engaging with the vendor and re-assessed annually thereafter.

> **Covered Security Criteria:** SOC2:2017.CC.9.2.2, SOC2:2022.CC.3.2, SOC2:2022.CC.9.2, SOC2:2022.CC.3.4,

Vendor Review

Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, and re-assess the vendors' security controls.

Covered Security Criteria: SOC2:2017.CC.9.2.2, SOC2:2022.P.6.4, SOC2:2022.CC.9.2,