WHISTLEBLOWER SECURITY

Information Privacy and Data Security

WhistleBlower Security's reporting and analytic solutions are combined with advanced security and data management to provide your organization with tools that will deter and prevent ongoing ethical concerns. Our data is housed in Canada, providing robust privacy legislation that prevents unauthorized access to this confidential information.

Key Features of WBS Data and Systems Security Protocols Include:

WhistleBlower Security systems and applications are available 24/7/365 via Microsoft Azure Cloud Services, providing our clients with:

- ISO 27001 Certified;
- Limitless scalability, reliability and business agility;
- Data security, privacy and control;
- The most up-to-date certified compliance with the most complex and evolving comprehensive set of attestations and accreditations;
- 100% compliance with key international and industry-specific compliance standards, including ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, SAA16 and SOC 1 and SOC 2;
- Rigorous third-party audits, by the British Standards Institution, Deloitte & Touche and others, that validate the adherence of MAC services to the strict requirements of these standards;
- Global Physical Infrastructure of servers, networks, data-centres and support.
- MS Windows Azure is certified ISO 27018 providing several important security safeguards;
  - » It ensures that there are defined restrictions on how personally identifiable information is handled, including restrictions on its transmission over public networks, storage on transportable media, and proper processes for data recovery and restoration efforts.
  - » This system also received confirmation from European data protection authorities that Microsoft's enterprise cloud contracts are in line with "model clauses" under EU privacy law regarding the international transfer of data.
- Back up data centre electronic integrity is maintained in conjunction with MS Azure cloud governance procedures and controls, summarized in the following points:
  - » ***Managing and controlling identity and user access*** to the environments, data, and applications by federating user identities to Azure Active Directory and enabling multi-factor authentication for a secured sign-in process.
  - » ***Encrypting communications and transmission processes.*** For data in transit, WBS, through MS Azure, uses industry-standard transport protocols between user devices and Microsoft data-centres, and within data-centres themselves and data is encrypted via industry leading SSL certificate at 2048-bit. For data at rest, WBS encrypts client and customer data at rest 100% of the time.
- Anti-virus protection is installed on all servers/ computers and is renewed regularly.
- The WBS platform includes automatic encryption of data and traffic and weekly server password changes are enforced for all developers and programmers.

- Systems are configured to check for anti-malware / anti-virus updates every 4 hours and install automatically.
- Intrusion Detection & Prevention System is used to identify, log, and block malicious activity such as: denial-of-service attacks, brute-force password-based attacks, identity spoofing, etc. All systems run on a redundant virtual and network infrastructure. In the event of a single hardware failure, our services continue to be operational. There is no downtime or data loss.
- WBS data is isolated from undesirable traffic and users by various security levels. WBS systems are setup with firewalled and partitioned networks to help protect against unwanted traffic from the Internet.
- The name of the Reviewer who may be involved in the incident will be excluded from the assigned auditor list and will not be able to review the case as the information is encrypted from view.
- WBS conducts an annual penetration testing by Pivot Point Security, a third party that conducts and issues a certification of completion and acknowledgement of zero vulnerabilities.

Global Regulatory Compliance

WBS is headquartered in Vancouver, Canada, offering its clients assurity that client confidential data will be well protected. Canada has one of the most active privacy regulatory enforcement environments in the world.

Our systems and applications are available 24/7/365 via Microsoft Azure Cloud Services, providing our clients with:

- WBS adheres to PIPEDA, FIPPA, and all privacy legislation both locally and globally.
- The EU officially recognizes the adequacy and strength of Canada's privacy legislation under Article 25 of the Privacy Directive for the EU
- WBS regularly monitors global regulatory environment to ensure compliance and implements measures to meet changing legislative requirements
- IAPP Member

WBS provided clients with additional features to meet Canadian data privacy regulations, including:

- Reporter data, collected via telephone, email, or through the WBS secure web portal is stored in a WBS designated and secured server.
- The name of the Reviewer who may be involved in the incident will be excluded from the assigned auditor list and will not be able to review the case as the information is encrypted from view.
- Only non-implicated primary Review Managers, assigned Reviewers, and the Reporter can review the case and relevant messages in the WBS case management system.
- Each client is assigned a unique ID for system use only. Data can only be accessed by those users who are attached to the unique ID.
- Firewall services use access control lists (ACLs) to permit and deny access into the WBS network. By default, all inbound traffic is denied and is only permitted when necessary.

FOR MORE INFORMATION

Contact WhistleBlower Security at 1-888-921-6875, email us at info@whistleblowersecurity.com, or visit our website at www.whistleblowersecurity.com