IntegrityCounts FAQs

WhistleBlower Security specializes in delivering flexible and modern 24/7/365 integrated Hotline and Case Management Ethics Reporting Services for public, private and not-for-profit organizations around the globe.

What encryption is used to secure data in transit or at rest?

All data / information transmission is done using encrypted methods. All incident report details are encrypted both during transmission and while at rest, and WBS maintains strict controls over who has access to systems that store confidential data. The information is encrypted using TLS between the client and the server. Once on the server the structured data is encrypted into an MS SQL Azure RDBMS using Transparent Data Encryption (AES-256). Any uploaded attachments are encrypted into Azure blob storage using Azure Storage Encryption. The certificates are managed at the platform level, allowing decryption only by the calling application and from specified hardware locations.

What are the details on the system technology?

WBS offers a Cloud-based, online case reporting and case management system.

The main technical features of the WBS system include:

- It is Cloud-hosted.
- The case management system is a fully integrate-able web-based system.
- It provides a full audit trail of historical and current reports.
- Data is encrypted in transit and at rest.
- It provides on-demand and customizable email notifications of all progress associated with each report as well as status updates.
- It provides a confidential and additional correspondence mechanism with the whistleblower enabling collaboration to ensure an efficient investigation.
- It provides a fully client-managed administration function to manage a company's authorized Reviewers' profiles and access to cases.
- It is scalable, customizable, and database expandable.
- It is equipped with the latest web-security and the industry's most advanced encryption technology

Are there audit trail capabilities?

WBS retains meta-data relating to the lifecycle of a case – audit log type information such as case events, time stamps and old and new values for updated fields.

The system also provides a full audit trail of historical and current records. The records are indelible to the users. Records can be deleted based on requests by the clients by the WBS development team or as required by regulations. WBS utilizes trace-based auditing and typically tracks the following:

- Login and logoff attempts
- Database server restarts
- Commands issued by users with less than client administrator privileges
- Attempted integrity violations (where changed or inserted data does not match a referential, unique, or check constraint)
- Update and delete operations
- Stored procedures executions "For internal developers tracking"
- Unsuccessful attempts to access the application (authorization failures)
- Changes to system catalogue table "For internal developers tracking"
- Row level and database operations "For internal developers tracking"

What about intrusion detection?

WBS maintains third party penetration testing of our platform annually and we have monthly automated vulnerability scan of our application end-points. Microsoft Azure also scan their host and virtual operating systems and physical and virtual infrastructure constantly.

Does the system provide a guaranteed availability of 99.9%?

WhistleBlower Security's *IntegrityCounts* reporting system supports many different organizations and each of these organizations has established and publicized how reports will be reviewed and by whom. Please review the communication material from your organization for specific details.

Are there corrective action processes to address system downtime issues?

The *IntegrityCounts* system runs on a redundant virtual and network infrastructure. In the event of a single hardware failure the application will continue to be operational. There would be no downtime or data loss. Recovery points for our databases are every 10 minutes (RPO) to protect against data loss / data corruption. We can restore from our recovery points within 30 minutes (RTO).

Additionally, our Cloud service provider, MS Windows Azure, maintains multiple data centres in Canada and ensures that data and applications are replicated and backed up to a minimum of two (2) data centres at any given time, which allows WBS to switch servers on demand and maintain operation 24 hours a day, 7 days a week, 365 days a year with data being restored in the original virtual servers within minutes.

Is there monitoring for and protection against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.)?

We educate developers to code defensively against common OWASP vulnerabilities. We require a code security review to be included in our code review process. We use SonarQube for SAST testing as well as Dependency Check for scanning for CVE vulnerabilities. We protect against XSS using the OWASP recommendations: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md

We protect against XSRF by including an XSRF token cookie using the Angular XSRF Feature: https://stormpath.com/blog/angular-xsrf

We protect against SQL injection by using prepared statements with parameterized queries, by using Stored Procedures where possible, whitelisting input validation and escaping user supplied input. We use Azure features and an Application Gateway to monitor, block and alert on specific traffic patterns that indicate malicious traffic.

Where is data stored?

All client data is hosted within Microsoft Azure data centres within Canada. The data is stored in Azure SQL databases and binary storage, logically separated from other tenant data.

All data is considered confidential and is encrypted using a 256-bit AES algorithm. Data can only be accessed (decrypted) through the client-facing web applications through controlled users access codes and pass-codes and, under a secured connection.

MS Azure data centers use maximum security protocols for physical safeguarding of their data center and use a variety of tests to electronically test the integrity of data and systems, please see link below:
https://azure.microsoft.com/en-us/support/trust-center/security/