Security & Privacy

IntelligenceBank is a secure, online information management platform, helping companies maximise the value of information.

As a web-based service that hosts and stores sensitive and business-critical information, the security and privacy of your information is our priority.

The following details technical security, redundancy and privacy standards that are pre-configured into the IntelligenceBank Service.

Encryption – HTTPS & SSL Transmission

IntelligenceBank offers its clients the capability to encrypt files stored within the system, as well as records in the Profile Database. This is implemented on a case by case basis, as encryption can affect speed of searches post encryption.

The IntelligenceBank platform has been digitally certified by GeoTrust 256-bit SSL (secure sockets layer). This ensures that when documents and data are transmitted over the open Internet, the information is unreadable by third parties. When a person tries to access a secured domain (i.e. your company's IntelligenceBank) an SSL handshake authenticates the server and establishes an encryption method and a unique session key. They can begin a secure session that protects message privacy and message integrity.

Virus Scanning

Virus scanning facilities can be made available on a client by client basis if required. The IntelligenceBank platform cannot be adversely affected by viruses located within files stored in the system, as file types are restricted to non-executable files.

Cloud Application Access - Web

Administrators of IntelligenceBank can easily ensure the service mirrors internal technical specifications and requirements, by customising how people access your IntelligenceBank. Specifically, Administrators can:

- Determine length, complexity and configurations of passwords.
- Set password reset timeframes.
- Set IP Address filters and restrictions.
- Set AD/SAML or LDAP login parameters – one and two legged authentication.
- Create conditions of entry (customised terms and conditions to use IntelligenceBank, which must be accepted upon logging in the first time).
- View login usage, logout and failed attempts with real-time reporting.
- Access a comprehensive audit trail of all actions conducted within IntelligenceBank – including views, downloads, edits and deletions.
- Automatically restrict access to user accounts which have entered the incorrect password too many times; these accounts can be unlocked later by the administrator if required.
- Automatically notify administrators when a user unsuccessfully tries to access his/her account.
- Receive confirmation if the email addressed used is incorrect and the user is locked out.
- Set roles and access levels by user group and/or by individual user.
- Enforce watermarking of a file with the user's name and date stamp.

All user and admin accounts are unique as they are tied to an email address. Review and authorisation is a responsibility of the end client. There are no 'default' accounts, and passwords can be configured to be changed during a time period.

Cloud Application Access – iPad App (if App enabled by client)

Each client can determine if they would like to allow their users to securely access files via IntelligenceBank's secure iPad App. The iPad App enables users to securely read and privately annotate files offline.

- All permission settings, password parameters and access levels are determined by the web based system – and the same password is used to access both.
- All files are encrypted on the IntelligenceBank iPad App.
- Text from a document cannot be copied and pasted from the iPad screen.
- All documents can be watermarked with a user's time and date stamp.
- Administrators can limit what users can do with a document – i.e. read online only, download document to iPad (outside of IntelligenceBank App), open document in other Apps, print from device.
- A separate security code for the IntelligenceBank iPad App can be enforced. If more than 5 attempts to login fail, all data is automatically wiped from the device.
- Timeout and password parameters (length, reset and complexity) can be set by Administrators.
- Time parameters for offline access without syncing to the web platform can be set.
- If an iPad is lost, access to files can be automatically removed for that user.

Firewalls

The IntelligenceBank servers are protected by separate hardware Firewalls, which deliver high-performance (so as not to inhibit speed of service) and multi-threat protection.

Redundancy, Uptime and Business Continuity

All data stored and managed within IntelligenceBank are hosted on dedicated high performance servers at Amazon EC2 and at Telstra, both in Australia. Telstra Cloud Data Centre(s) are located in Australia and are ISO 27001 certified.

When Hosted by IntelligenceBank, your information is backed up nightly on a separate dedicated server 'onsite'. In addition, your data is incrementally backed up each night to a dedicated 'off site' data centre. Backups are stored both on site (for rapid access in a non-disaster situation) and off site (for disaster recovery).

The main application server has full disk level backups, for rapid recovery if a bare metal restore is required.

If the main application server is not available for technical reasons, IntelligenceBank can create a new instance of your platform within 2 hours if required, using data that is less than 24 hours old.

If new features are rolled out and present a problem, IntelligenceBank's code can be instantly rolled back.

Confidentiality

Upon becoming an IntelligenceBank client, we will enter into a confidentiality agreement with you, as at times, your dedicated Account Manager or Technical Support personnel may be required to access your IntelligenceBank, at your request. Client administrators receive full reporting transparency, of data accessed. We only access your platform, once you provide us with access.

Technology

IntelligenceBank is a proprietary SaaS (software as a service) application, which has been developed using PHP software, MySQL & XML databases and Unix servers. The software is browser independent, but has been designed for Internet Explorer 8+ and the latest versions of Chrome, Firefox and Safari.

External Penetration Testing

IntelligenceBank has been audited by PureHacking, an external penetration testing company. The external auditor was not able to 'hack' into IntelligenceBank, and supplied IntelligenceBank with a list of low priority recommendations, all of which were immediately addressed. Note the only "Medium" risk item is due to the capability for IntelligenceBank clients to set their own password parameters, depending on the clients' requirement. Due to the different uses of IntelligenceBank, we have left this capacity within the system.

Security and Monitoring

Server Level

- A hardware firewall, with intrusion detection and reporting, restricts access to the IntelligenceBank servers.
- Continuing monitoring of core services (HTTP, HTTPS, Database, DNS, Search and Conversion services, etc.)
- Intrusion detection monitoring at server level.
    - Tripwire monitors server level configuration for unauthorised changes.
    - Logcheck monitors system logs for unusual activity, including all access to monitored system.
    - Tiger monitors changes to available services and additional configuration checks.
- Suhosin, a hardened PHP version, is used to run the main application.
- Server OS patches are checked daily and applied as appropriate.
- Only dedicated servers are used (no shared servers).
- Secure hosting is provided by Amazon in Australia and in the United States (hosting location is based on your location for optimal performance) which are ISO 27001 certified.

Security considerations within the application design:

- Server data storage; cookies are only ever used to store session identification tokens, not for any other data.
- Secure session information
    - Session information is only ever transmitted through cookies, not through GET or POST parameters.
    - Session information is only ever transmitted over HTTPS, never over HTTP.
    - Session cookies use the HTTP Only flag; all modern browsers (including IE6 SP1) will prevent this session information from being available to JavaScript, as a protection against XSS.
    - Session hijacking detection is used to automatically log out users if suspicious behaviour is detected.
- Secure data transmission; HTTPS is required for all communication and clients connecting over HTTP will be redirected to the appropriate HTTPS site.
- All IntelligenceBank access goes through a single controller, which checks all accesses against the configured ACLs.
- The OWASP ESAPI project is used to enforce data integrity, both on input and on display to the user
- Prepared statements with the PHP PDO library are used for database access, removing the risk of SQL Injection attacks.
- Client resources are stored outside the web server root, preventing direct access.
- Passwords are salted and encrypted before storing in the database; even in the case of a system compromise, the passwords will be relatively difficult to crack.

SLA's

SLA's include 99.9% uptime guarantee, access 24/7/365. Response time for critical issues is 1 hour. Response time for non-critical issues is 4 hours. Response time for non-critical customer support is a business day.

Customer Support

Support Service	Description	Performance Measure	Service Level (measured monthly)
Admin Support	Provision of a single point of contact for user support requests during the hours of operation 9am to 5pm AEST, (*excluding public holidays*).	Responded to within [*4* hours] during hours of operation	90%
Technical Support	Provision of a single point of contact for logging and tracking of incidents affecting service delivery during the hours of operation 24x7 excluding scheduled maintenance.	Responded to within [*1 hour*] [during hours of operation]	90%

Disaster Recovery

In case of a Disaster, the ASP service recovery time objective (RTO) applies, and specifies from which time onwards client users can recommence using the Application via the ASP Service.	RTO is [24 hours] from time of Disaster	100%

In case of a Disaster, the recovery point objective (RPO) limits the maximum data loss to client users. The RPO specifies the point in time prior to the Disaster from which all data must be recovered and available to client users using the Application via the ASP Service.	RPO is [24 hours] prior to Disaster	100%

Disaster Recovery Performance Measures

Incident Severity	Definition	Example	Performance Measure				Service Level (Measured monthly)
			Initial Response to Client	Feedback to Client until service is restored	Target Time – restoring service	Target time – performance fix applied	
1	**Critical Impact** – Includes all incidents, which have a major impact to the ASP Service, where no workaround is in place.	- A service is totally unavailable.	Immediate	Every 1 hour	4 hours	5 Business Days	100%
2	**Serious Impact –** Includes all incidents which have a major impact on delivery of a significant part of the ASP Service or are likely to progress to total loss of ASP Service to Client	- A service is significantly impaired. - One or more core functions of a service are unavailable	1 Hour	Every 2 hours	4 hours	10 Business Days	100%
3	**Local Impact –** Includes all incidents which require attention, but have no major or impending impact on delivery of full ASP Service to Client	- An incident is causing minimal impact but has created a risk to a service and is required to be resolved to prevent a follow on impact to service	24 hours	Every 48 hours	1 week	4 weeks	90%
4	The recovery point objective (RPO) limits the maximum data loss to Client users. The RPO specifies the point in time prior to the incident from which all data must be recovered and available to Client users using the Application via the ASP Service.		RPO is 24 hours prior to incident				100%

Physical Security – Data Centres

All IntelligenceBank data centres are ISO 27001 certified for Security Management. Amazon has been certified to AS/NZS 31000:2009 Risk Management Standard, and is also ASIO T4 accredited and provides a 24/7 monitoring and incident response capability.

Other physical security features include network and server firewalls, Managed Internet Gateway, Internet Protection, Denial of Service Protection, remote access security, disaster recovery and backup/restore. It also includes:

- On-site security personnel – 24/7.
- Electronically-secured floors with access restrictions.
- CCTV surveillance for corridors and rooms hosting ICT infrastructure.
- Secure ICT infrastructure, including locked cabinets and cages.
- Power and connection redundancy.
- VESDA Fire Protection.
- All servers are racked appropriately with space guidelines between servers.
- Our data centre is not located in a flood zone and there is N+1 power redundancy.
- Onsite engineers provide scheduled server maintenance as well as 'on-call' assistance should an issue occur. Spare parts are maintained on site and contracts are updated accordingly.

Proactive Monitoring of Application and Data Centres

IntelligenceBank pro-actively monitors its operating system, core functions, up time, patch upgrades, firewall status and hacking attempts. Alerts should any of these issues arise, automated email alerts are logged and are generated at 5-minute intervals. All issues are addressed immediately, and issues are logged within our internal reporting system with remedy, timing and verification.

Our security policy is reviewed each quarter by development team and board.

IntelligenceBank assesses security breaches and risks on going, as well as formally on a quarterly basis.

IntelligenceBank has also product insurance for IT related risks.

Staff Security Controls

All core references are checked prior to employment.

Staff sign confidentiality clause as part of employment agreement.

Staff are briefed on secure nature of data and only given access at level required to complete their role.

Our development and client fulfillment systems contain a transparent audit trail for our clients, so at all times, we have visibility as to which person has logged into the platform. Third party contractors can only access portions of the front end systems with prior agreement and with short-term accessibility passwords. Contractors are not given access to primary code repository nor client fulfillment system.

When staff leave IntelligenceBank, their system access is revoked and user names removed. Any passwords that person may have had access to are changed, and their email is forwarded to HR.

Contract Termination Procedure

When a contract is terminated, for the agreed upon fee, IntelligenceBank will provide the client with a backup of all files on disc. Once the client has confirmed they have received all files in writing to IntelligenceBank, and the contract date has expired, IntelligenceBank will permanently wipe all primary and backup data. A letter confirming the deletion of client data will be sent to the client.

Media and Data Security Disposal

IntelligenceBank stores the data within its secure platform, using SSL, and at no time handles the actual data unless client personnel are advised prior. Lables are not placed on provided media. Media remains in IntelligenceBank's office only whilst being transferred to servers, and then is returned and/or shredded if required.

Data is removed from media once installed into IB system, and data is erased using Secure Removal methods of OS.

Change Management

IntelligenceBank's cloud based service is continually upgraded, at regular periods (second and fourth Monday of each month). Our end-user clients may choose to enable or disable most of the features that are deployed.

All clients are notified at least 5 days prior to new major features and bug fixes. Usually changes do not require downtime, but if scheduled downtime is required, clients are notified in a timely manner, and a message to end users about the schedule downtime is displayed on the platform.

All changes are deployed on test systems first, and prior to rolling out significant new features, penetration testing is conducted on the system.

All code is regularly checked into a code repository system, whereby changes can be instantly rolled back if required.

Emergency change management processes are also in place, including roll-back functionality.

Our technical staff are on 24/7 standby.

Server build and security standards are documented and new systems are built using those guidelines.

Penetration testing is conducted regularly using an externally recommended software programme. Any findings from this penetration testing are immediately actioned.

Network Security

The server security is based on a shared nothing infrastructure. Each server has its own firewall, which is configured to only allow access as appropriate for its particular service.

Only the web server is configured for public access. Database and search servers are accessible only via the internal network between the servers, and not addressable via the public Internet. The database and search servers are accessible by specific external IP addresses only, for application and service monitoring and troubleshooting.

Each client can be provided with periodical reports of what access is available through the firewalls – however; this will incur a nominal fee.

24 x 7 monitoring is enabled using an external self-managed monitoring service.

The external facing infrastructure has been penetration tested using the BurpSuite from PortSwigger, one of the most highly regarded penetration testing tools. The tests are run by the internal team on a bi-monthly basis.

Incident Reporting

All major incidents, including hardware failure, Internet service delivery failure and major (successful) firewall attacks are communicated to clients as they are known.

IntelligenceBank's CTO confirms the nature of the incident, and IntelligenceBank's account management team communicates this to all affected clients. When the situation is resolved, all clients receive a confirmation email.

Any significant outages and or attacks are raised with the IntelligenceBank board and senior management.

System Patches

System patches and security patches are notified to IB and they are installed first on test servers. They are then immediately deployed once the test is passed.

The majority of our code has unit testing, so if there is a fix/patch that will adversely affect the system, we will be automated prior to launching. Note – however, no deployments can be guaranteed to be 100% bug free.

Data Sovereignty

Depending on client requirements, all data and backups can be hosted in either the US, or Australia.