



Technology and Privacy Brief

This Technology and Privacy Brief is intended to give you a transparent understanding of the technologies and policies related to data security at Better Impact to help you determine whether we are good fit for your organisation.

If you require additional information and would like us to fill in a custom questionnaire, we will be happy to do so, but given how inexpensive our software is (including unlimited administrators, all software, data hosting, software upgrades and 24x5 support), we hope you understand we would have to charge for this service where the annual fees are estimated to be under \$10,000.

Fewer than 2% of our members request services such as these so we have not incorporated any time for them in determining our subscription fees. This is one of many steps we take to keep the cost of our software geared toward the needs of not-for-profit organisations.

Questions regarding the information here can be directed to houston@betterimpact.com.au

Table of Contents

BETTER IMPACT PRIVACY PRINCIPLES	4
A.1 WE PUT A HUMAN FACE TO PERSONAL DATA	4
A.2 WE THINK AHEAD	4
A.3 WE MAKE PRIVACY EVERYONE’S BUSINESS	4
A.4 WE KEEP IT OPEN, FLEXIBLE AND PRIVATE	4
A.5 WE COMMIT TO CONTINUAL IMPROVEMENT	5
A.6 WE ARE RESPONSIBLE AND COMPLIANT	5
A.7 WE COLLECT ONLY WHAT IS NEEDED	5
A.8 WE ARE MOTIVATED TO HELP	5
THE APPLICATION	6
B.1 ARCHITECTURE	6
B.2 APPLICATION DEVELOPMENT	6
B.3 RELEASE CYCLES	7
B.4 SYSTEM REQUIREMENTS	7
B.5 API PROTOCOL	7
THE DATA CENTRE	8
C.1 LOCATION	8
C.2 PHYSICAL AND ENVIRONMENTAL SECURITY	8
C.3 REDUNDANCY	8
C.4 CERTIFICATIONS AND ACCREDITATIONS	9
C.5 THIRD-PARTY VISITS	9
DATA PROTECTION - CONTROLS	10
D.1 CRYPTOGRAPHIC CONTROL	10
D.2 ACCESS CONTROL	10
D.3 PASSWORD REQUIREMENTS AND MANAGEMENT	11
D.4 NETWORK SECURITY AND ASSURANCE	11
D.5 SOFTWARE TESTING AND TEST DATA MANAGEMENT	12
D.6 PROTECTION FROM MALWARE	12
DATA PROTECTION - GOVERNANCE	13
E.1 PERSONNEL	13
E.2 CERTIFICATIONS AND ACCREDITATIONS	13
E.3 RISK MANAGEMENT	13
E.4 INFORMATION SECURITY GOVERNANCE	14
E.5 CHANGE MANAGEMENT PROCEDURE	15
E.6 KEY ADMINISTRATIVE POLICIES	15
E.7 INCIDENT MANAGEMENT	16
E.8 SECURITY AND PRIVACY AWARENESS TRAINING	16

HIGH AVAILABILITY, RESILIENCY AND RELIABILITY	17
F.1 CAPACITY MANAGEMENT	17
F.2 DISASTER RECOVERY AND BUSINESS CONTINUITY	18
DATA PORTABILITY AND DESTRUCTION	19
G.1 DATA DESTRUCTION	19
G.2 CLIENT-MANAGED DATA EXPORT/POST-SUBSCRIPTION DATA ACCESS	19
REMOTE / MOBILE ACCESS	20
H.1 IP RESTRICTIONS	20
H.2 MOBILE DEPLOYMENT AND SECURITY	20
THE AUSTRALIAN PRIVACY PRINCIPLES	21
I.1 CONSIDERATION OF PERSONAL INFORMATION PRIVACY	21
I.2 COLLECTION OF PERSONAL INFORMATION	21
I.3 DEALING WITH PERSONAL INFORMATION	21
I.4 INTEGRITY OF PERSONAL INFORMATION	21
I.5 ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION	21



Better Impact Privacy Principles

Over the years, we have remained consistent in prioritising data protection and privacy in our business. Our presence in multiple jurisdictions and the requirement to comply with privacy regulations necessitated creating a privacy compliance program with elements of all applicable regulations. Beyond regulatory compliance however, we recognise that the core drivers of our privacy practices align with our organisation values and business objectives.

Privacy is ingrained into all aspects of our product design and customer engagements. The following Better Impact Privacy Principles are the core drivers of our privacy practices. These principles are derived from years of experience in providing secure data storage, fair and transparent information processing practices and compliance with multiple privacy regulations.

A.1 We put a human face to personal data

People are at the heart of our privacy practices. We don't just process or store personal data; we consider that we are dealing with real people (data subjects in data privacy jargon) and that we owe it to them to protect their data.

A.2 We think ahead

We think ahead and solve problems in advance of their occurrence. Our systems, development processes, business practices and organisation ethics reflect the premium we place on privacy. The foundation of our work and business is built on the consciousness that we handle sensitive information that must be protected throughout its lifecycle. We envisage a privacy breach and put necessary controls in place to prevent its occurrence. Our risk management process takes privacy into account in the risk assessment methodology and risk treatment plan.

A.3 We make privacy everyone's business

While we have dedicated personnel on the Better Impact team who are responsible for privacy, the work of maintaining privacy of information is the duty of every member of the team. This responsibility is clearly communicated as a member joins the team and is reinforced with ongoing privacy training provided to all staff on regular basis to keep abreast of privacy best practices.

A.4 We keep it open, flexible and private

We follow a transparent approach to information processing. All stakeholders have access to their information. Subject to the data retention policies provided by our members to their end users, they are in control of their information. However, we maintain strict access control that restricts access to information such that end users have access to their information only, and in the case of volunteers and Client Impact, only to associated clients.



Better Impact Privacy Principles

A.5 We commit to continual improvement

We make effort to attain perfection, but we recognise that this is a near impossibility. Therefore, we take advantage of every opportunity to get better on a continual basis. We never let go of an opportunity to improve a privacy practice. While every effort is made to ensure that we do not record a privacy breach, we have plans in place to learn from privacy-linked incidents should one ever occur.

A.6 We are responsible and compliant

Our business operates in multiple jurisdictions serving clients around the world. In handling data, we recognise that we are subjected to a variety of legislations and requirements on data privacy and protection. Our dynamic compliance program is built around continual compliance with all applicable legislations.

A.7 We collect only what is needed

We will only collect necessary information minimally required to fulfil the purpose for which it is collected. Limiting collection helps us focus resources on adequate protection.

A.8 We are motivated to help

We share knowledge freely with our members through privacy advocacy and training programs. We support our members in embracing safe data privacy and protection practices. We continually seek ways we can help them improve their approach to information security by encouraging them to adopt our principles or come up with their own.

The Application

B.1 Architecture

- Multitenant SaaS
- **Data segregation**

Each user is identified by a unique username which they use in conjunction with a password for login purposes. Internally the user is assigned a unique numerical ID used as a primary database key. Access to shared information is restricted by using joins against the primary user field to ensure the user has access only to appropriate records. Data security profiles are handled directly in the database in addition to the Business Logic Layer which exposes data services to the UI Layer.

B.2 Application Development

- **Development tools**
 - ASP.NET MVC 5
 - VB.NET
 - JQuery/ JQuery mobile / JSON / Ajax
 - NHibernate
 - SQL server
- **Development personnel**
 - All aspects of our software development are completed by Better Impact developers who are full-time employees. Our software development is fully internal (no outsourcing or subcontracting).
 - All source codes to our propriety products are owned by Better Impact and they remain our intellectual properties.
- **System design and secure development principles**
 - Security is planned and entrenched in all processes involved in our system lifecycle from requirement gathering to design, development, testing and live deployment. Our change management procedure also ensures that the confidentiality, integrity, and availability of our vital information is always assured.
 - Our software products are designed using best-practice and principles in secure web application development:
 - Our clients handle a great deal of Personally Identifiable information (PII). We recognise the importance of privacy when handling PII and incorporate a privacy and security by design approach to ensure users information are protected and kept away from other users of our applications. We do not use personal information for testing.
 - Open Web Application Security Project (OWASP) Principles: Our application design follows the principles of secure development that mitigates all the common risks of web application including but not limited to:
 - Injection flaws
 - Broken Authentication
 - Insecure Deserialisation
 - Broken Access Control

These principles are followed for all our development and software change projects.

The Application

- **Integrity Controls**
 - OWASP
 - Microsoft Security Development Lifecycle

B.3 Release Cycles

- **Major releases:** Every 4-5 years (12 hours downtime, typically starting around 01:00 GMT)
- **Minor releases:** Every 8-10 weeks (1 to 15 minutes downtime, typically starting around 02:00 GMT)

B.4 System Requirements

- **Protocols and ports requirement for connectivity**
 - HTTP on port 80
 - HTTPS on port 443
- **Browser and operating system requirement**
 - Any modern browser, Internet explorer 11 or later, Edge, Safari, Chrome, or Firefox. JavaScript must be enabled.
 - Runs on any operating system that supports web browsers on windows or MacOS- based systems.
- **Mobile**
 - Application is available as web app (responsive) and native app in Android and iOS versions.
 - Native apps are available in [Google Play Store \(Android\)](#) and [App Store \(iOS\)](#)
 - Minimum OS version required: Android 7.0 and iOS 11.0

B.5 API protocol

- Passive RESTful
- More technical information about API available through the links below:
 - [API](#)
 - [API Keys](#)

The Data Centre

C.1 Location

- **Live Data**
Aptum Technologies (www.aptum.com)
20 Pullman Court
Scarborough, Ontario M1X 1E4
Canada
- **Backup Data**
Aptum Technologies (for rapid restore if needed)
- **Offsite Backup**
Thrive Network Inc. (www.thrivenextgen.com)
151 Front Street West
Toronto, Ontario M5J 2N1
Canada
- **DRaaS Site**
Thrive Network Inc. (www.thrivenextgen.com)
3500 Rue F.X-Tessie,
Vaudreuil-Dorion, Quebec, J7V 5V5
Canada

C.2 Physical and environmental security

- **Video surveillance:** Cameras throughout the premises and on the exterior
- **Network Operations Centre:** 24x7x365
- **Physical access controls:** Key cards, biometric controls. single person mantrap doors

C.3 Redundancy

- **Power feed**
Diesel generators supply the redundant power and there is on-site fuel storage capacity for 48 hours at full load. Generator redundancy is N+1. In the event of an outage of the main utility feed all generators will start up automatically and take over the full building load.
- **HVAC system**
 - Closed chilled water loop
 - Chiller plant with cooling towers feeding Liebert CRAH units.
 - On site well for redundant water.
- **Fire suppression:** Pre-action dry pipe system

The Data Centre

C.4 Certifications and accreditations

- ISO/IEC 27001
- ISO 9001
- CSAE 3416
- SOC 2 Type II

C.5 Third-party visits

- Prearrangement through Better Impact is required.

Data Protection – Controls

D.1 Cryptographic control

- **Encryption algorithms**
 - Data in Transit: TLS 1.2 ECDHE RSA with AES 256bit
 - Live data at rest: 256 BIT AES encryption
 - Passwords at rest: One-way hashing algorithm (bcrypt) with a random salt value
 - Backup data rest: 256 BIT AES encryption
 - SSL certificate hashing: SHA-384
 - All versions of SSL and older versions of TLS, specifically TLS 1.0 and TLS 1.1 are disabled.
- **Encryption Key Management**
 - Decryption keys for data at-rest on our database server are stored in a FIPS-compliant double encrypted profile on the server.
 - Offsite electronic backups of the encryption key for at-rest data are stored on FIPS-compatible secure USB keys
 - Where a key is suspected to have been compromised, the affected database is decrypted and re-encrypted with new keys generated
 - As a multitenant SaaS offering, our clients are not allowed to manage their own keys

D.2 Access Control

- **Brute force penetration lockout**
 - Ten unsuccessful attempts within five minutes on the same username lock out that username for 10 minutes.
 - Internal administrators can reset a user.
- **Log of log-on attempts**
 - Successful and unsuccessful attempts – retained for ten years
- **Admin user session lockout after a period of inactivity** – Default Session timeout is 30 minutes. However, this is configurable to 10 - 240 minutes
- **Permission-based identities with different levels of access to functions** – Configurable
- **Access to networks and network services**
 - Access to the Better Impact network is granted on-premise in line with our access control principles.
 - Remote access to the network is granted via Virtual Private Network (VPN) on a need-to-use basis.
 - VPN access is granted via an approval process and is strictly monitored.
 - Two-factor authentication is utilised (where possible) for some service access.
 - Suppliers are not given access our network.
- **Review of User Access Rights**
 - We regularly review user access right to ensure appropriate system access is maintained
- **Access control to program source code**
 - Access to Better Impact proprietary software source code is strictly controlled to maintain its confidentiality, integrity, and availability always.

Data Protection – Controls

D.3 Password requirements and management

- **Better Impact staff**
 - Passwords must contain a minimum of 12 characters and include at least 1 uppercase, 1 lowercase, 1 numeral and 1 special character.
 - Two factor authentication and brute force protection are in place.
Password must not be one of the passwords in the global dictionary of common passwords
- **Organisation administrators**
 - Passwords must contain a minimum of 12 characters and include at least 1 upper case letter, 1 lowercase letter and 1 number.
 - Brute force protection is in place providing an additional guard against hijacking.
 - Two-factor authentication is available as a free option.
 - Password must not be one of the passwords in the global dictionary of common passwords.
- **Organisation constituents**
 - Passwords must contain a minimum of 12 characters and include at least 1 upper case letter, 1 lowercase letter and 1 number.
 - Brute force protection is in place providing an additional guard against hijacking.
 - Password must not be one of the passwords in the global dictionary of common passwords.
- **Periodic changes of passwords**
 - Not enforced as per [NIST recommendations](#).
- **Password changes required after password reset**
 - Required as part of the first log in after the creation of a profile by an administrator, the reset of a password by an administrator, or the automated password reset triggered by an administrative or constituent user.

D.4 Network security and assurance

- **Web Application Firewall**
 - Fully automated monitoring
 - Allows for virtual patching
 - Automated blocking
 - Automated alerting
- **Vulnerability Scanning**
 - Internal and external scanning
 - Proactive automated scans against emerging threats
 - Weekly scheduled scans
- **Third party penetration tests**
 - Typically conducted annually and not more than 18 months apart – report available on request
 - Last test – June 2025
- **Customer-arranged penetration tests:** Allowed with advance scheduling. Fees for our time may apply.
- **Remote secure network access**

Data Protection – Controls

- VPN with no Dual-homing / split tunneling

D.5 Software testing and test data management

▪ Test and production environment

- Distinct systems
- Testing is conducted in our development environment, which is logically and physically separate from our production environment.

▪ Test data

- We do not use production data for testing.
- Our test data are randomly generated and do not contain any personally identifiable information linked to a natural person

D.6 Protection from malware

- **Application and database servers:** ESET antivirus for Windows Server (updated automatically)
- **Development computers** - ESET endpoint antivirus (updated automatically)
- **Non-development workstations:** Bitdefender antivirus (updated automatically)
- **Security patches:** Critical patches are applied as issued by any vendor. Noncritical patches are applied monthly
- Centralized management and reporting

Data Protection – Governance

E.1 Personnel

- **Privacy Officer:** Houston Goodwin - houston@betterimpact.com.au
- **Compliance and System Specialist:** Adeyinka Jegede – adeyinka@betterimpact.com.au

E.2 Certifications and accreditations

- **Organisation**
 - **ISO/IEC 27001:2022**
 - Certificate number: CERT-000160
 - Certified since: 2021-09-30
 - Valid until: 2027-09-29
 - **ISO/IEC 27017:2015**
 - Certificate number: CERT-000161
 - Certified since: 2021-09-30
 - Valid until: 2027-09-29
 - Copies of certificates available at www.betterimpact.com.au/ISO
- **Personnel**
 - ISO/IEC 27001 LI
 - CISA
 - CDPSE
 - CBAP
 - CVA
 - COBIT-5

E.3 Risk Management

- **Risk identification**
 - Our security policies and practices conform with the requirement of ISO 27001. We identify risk through a combination of activities including:
 - Brainstorming and interviews with process and risk owners
 - Desktop research and business plan review,
 - Asset inventory through interviews with asset owners
 - Existing process review leading to a documented risk register.
- **Risk analysis and evaluation**
 - Having identified the risks, relevant risk scenarios are added to the ISO 27001 risk register and treatment plan in the ISMS.online platform used to manage our ISMS.
 - Risks are relevantly described with a simple reference for whether they are internal, external or both. Every risk has an owner, yet each risk can have composite treatment areas delivered by the same or other people as set out in the relevant risk treatment plan.
 - Relevant documents are produced as evidence to auditors and internal stakeholders that appropriate action has been taken.

Data Protection – Governance

- Risk register is updated and reviewed based on the defined intervals and nature of risks.
- ISMS Board members and risk owners are notified of changes made to the risk register.
- **Risk assessment and treatment**
 - We conduct a risk assessment of our information assets and processes in line with ISO 27005 and ISO 31000. Our security controls reflect the results of our risk assessment and are carefully chosen in line with our unique business requirement, best practices, and the recommendations contained in ISO 27002 and 27017:2015.

E.4 Information security governance

- **Information security policy**
 - Our Information Security Policy presents the leadership commitment to information security and overarching policy statements to which all subordinate policies adhere.
 - The **ISMS** is the Information Security Management System, documented and communicated through isms.online. It has been designed in accordance with the specifications contained in ISO 27001:2022 and controls recommended in ISO 27002, and ISO 27017:2015.
 - Subordinate policies include, but are not limited to the following:

1. Acceptable use of assets	19	Information security policy
2. Access control	20	Information security review
3. Asset management	21	ISMS internal audit
4. Back-up and restore	22	ISMS management review
5. Business continuity plan and policy	23	Mobile device policy
6. Classification and labelling of information	24	Password policy
7. Clear desk and clear screen	25	Patch management
8. Cryptographic control	26	Physical and environmental security
9. Disposal of media	27	Privacy and protection of personally identifiable information
10. Documented information management	28	Restriction on use of privileged utility programs
11. Equipment maintenance	29	Review of Information security
12. Error handling	30	Risk management and treatment process
13. Human resources security	31	Secure disposal and reuse of media & equipment
14. Improvement and corrective action	32	Software update
15. Information and Media Transfer	33	Supplier (and other important) relationships
16. Information Security Incident Management	34	User acceptance testing
17. Information security policy for supplier relationships <ul style="list-style-type: none"> ▪ Information and communication technology supply chain ▪ Information security within supplier agreements 	35	Operations security policy <ul style="list-style-type: none"> ▪ Back-up ▪ Capacity management ▪ Malware control ▪ Technical vulnerability management
18. Network and communication control <ul style="list-style-type: none"> ▪ Confidentiality and non-disclosure agreements 	36	Secure development policy <ul style="list-style-type: none"> ▪ Secure development environment ▪ Secure system engineering principles

Data Protection – Governance

<ul style="list-style-type: none"> ▪ Security of network services ▪ Securing application services on public networks ▪ Segregation in networks 	<ul style="list-style-type: none"> ▪ Security and privacy in testing ▪ System change control ▪ System security testing ▪ Technical review of application after platform changes
---	---

- **Security policy review and communication**
 - Our security policies are reviewed at least annually, or whenever a significant change occurs that would give reason to review and potentially change a policy.
 - All staff have access to our security policies through the isms.online environment.
 - They are required to read and acknowledge that they understand the content.
 - Our policies are concise, clear, and promptly communicated to relevant staff.
- **Roles and Responsibilities in Information security**
 - We demonstrate leadership and allocate roles in accordance with the requirements of ISO 27001:2022
 - We have a management review board called the ISMS Board made up of the senior management team that sits over the ISMS. Collectively this body takes the main strategic decisions around information security and issues affecting performance. The board is chaired by the CEO

E.5 Change management procedure

- Changes considered are reviewed by the technical team
- Technical team lead signs off on changes
- Database and business rules programming is completed
- Front end developers code as required
- Automated and manual testing occur in the test environment
- Users are advised of changes a week ahead of launch
- System changes are uploaded to the live environment

E.6 Key administrative policies

- Contracts of employment impose an obligation on employees to comply with data protection and confidentiality policies
- Criminal background checks are processed on all employees
- Annual staff review of documented information security policies to guide personnel in system access and security
- Clean desk / clear screen policy
- Role-based access control (RBAC) and the principle of least privilege
- Access to client data provided to staff on a need-to-know basis
- Client data sharing (not allowed)
- Security incident response plan
- Business continuity plan
- Client notification if we receive a request for personal information (2 business day window)
- System access privileges of terminated employees revoked as a component of the employee termination process

Data Protection – Governance

E.7 Incident management

- **Data breach incident response**
 - Step 1 – Identify and contain
 - Step 2 – Notify all staff immediately and clients within 24 hours*
 - Step 3 – Investigate
 - Step 4 – Notify all staff and clients*
 - Step 5 – Implement change
 - Step 6 – Notify all staff and clients*
 - *Clients will be notified via email to those listed as administrators in the system

- **Security breaches / loss or unauthorised disclosure of personal data since 2001 (launch of the software)**
 - None

E.8 Security and privacy awareness training

- A review of general best practices and key practices related to our specific environment is administered annually.
- Topics include policy review and updates, compliance standards review, the importance of adherence to confidentiality policy, what constitutes confidential information, and phishing and social engineering awareness, handling personal data securely and general information security best practices.
- Regular training on applicable privacy regulations including the Australian privacy principles.

High Availability, Resiliency and Reliability

We ensure that our systems maintain high availability, remain reliable and continual resilience even in the event of service disruptions. We deploy resources for improved availability and efficiency of our service. These include disk space monitoring, bandwidth management, uptime monitoring and other measures that ensure we never disappoint our clients.

F.1 Capacity Management

- External and internal monitoring for infrastructure and external monitoring for network endpoint availability, and for application health metrics.
- CDN to serve static content in a redundant and performant manner. This will ensure our application assets are loaded quickly world-wide
- Two DNS providers for our core services to prevent against DNS DoS attacks and other service impact involving a single provider.
- We do not store video or any large media content. Individual file sizes are limited depending on context (maximum 10MB).
- Infrastructure maintenance is typically scheduled on off-peak hours (weekends and evenings). A minimum notice of 24 hours for service-impacting maintenance and a history of our maintenance and uptime are provided on our status page at <https://www.betterimpactstatus.com/>
- Maintenance includes OS and application patches, hardware upgrades, network configuration changes, server replacements/additions and deployments of our application.

- **Uptime**
 - Guaranteed in our SLA (excluding planned maintenance): 99.95%
 - Historic uptime: 99.997% over the past nine years

- **System redundancies**
 - Our system is N+1 across the entire system except the database server.
 - Full hardware redundancies with automated failover.

- **Fail-over procedures**
 - Replacements for all hardware are readily available within our data centre with a 1-hour SLA.
 - Data is backed up onsite for faster restoration if available (and on offsite for broader protection).

- **Throughput limit**
 - We do not set a throughput limit on our service.
 - Throttling is not applied.
 - Our highest number of concurrent users to date is more than 7,500.
 - We monitor server resources continuously and upgrade well ahead of the demand curve

High Availability, Resiliency and Reliability

F.2 Disaster Recovery and Business Continuity

- **Backups**
 - Full backup once per week
 - Incremental backup once per day
 - Transaction log backup once every 15 minutes
 - 14 days retention
 - Full restoration automatically tested weekly
 - Backups are for full system restoration only
 - Full image level backups of all systems are taken daily

- **Disaster Recovery as a Service (DRaaS)**
 - We use Disaster Recovery as a Service (DRaaS) to ensure reliable service continuity during unexpected disruptions. DRaaS replicates our critical systems and data in real-time to a secure cloud environment, enabling rapid failover and recovery.

- **Recovery Point Objective (RPO): 15 minutes**

- **Recovery Time Objective (RTO)**
 - 1 hour on hardware failure (if redundant hardware fails simultaneously)
 - 48 hours in the event of a disaster at our primary data centre that requires failover to our secondary site.

- **Business continuity plan**
 - We have a comprehensive Business continuity plan and policy which always assure the continual availability of our service. The business continuity plan is to prepare the team in the event of extended service outages caused by factors beyond control and restore services to the widest extent possible in a minimum time frame.

 - The BCP addresses the following:
 - Clearly defined business continuity objectives
 - Plan for regular testing of BCP to ensure it remains practical and effective
 - Role and responsibilities in the business continuity are assigned and documented
 - The plan is being continually improved
 - Events are classified into major and minor events
 - Responses are appropriate to the event type
 - Event communication plan
 - Clearly defined disaster recovery plans and procedures

Data Portability and Destruction

G.1 Data destruction

▪ **Server**

- Clients can delete all their data except contact details.
- Upon request, we will delete all contact details except for users who have an association between their MyImpactPage.com profile and another Better Impact client. Their details need to be preserved for the end user to use elsewhere.

▪ **Backups**

- Data deleted from the server is destructed 15 days after deletion from the server.
- Our backup retention period is 14 days. Data deleted from the server will be out of the backup retention area automatically after that time.

▪ **Hard drive**

- If the disc is still functioning, SQL field deletion.
- If the disc is no longer functioning or its use has been discontinued, there is a defined process for wiping and degaussing information.
- Certificates of destruction with drive serial numbers are available when applicable

G.2 Client-managed data export/post-subscription data access

- Clients can download their data any time during the subscription period.
- Clients can delete or request deletion of their data upon agreement termination.
- Where clients choose to retain their data in our system, access and retention are guided by applicable legal and regulatory obligations

Remote / Mobile Access

H.1 IP restrictions

- **Mobile use restriction by IP address**
 - Available for the recording of volunteer hours
 - Not available for other non-administrator functions
 - Available for administrative function via IP address restrictions
- **Administrative access restriction by IP address**
 - Available (Additional fees apply)

H.2 Mobile deployment and security

- **PIN or password protection on mobile devices**
 - Required
- **Client confidential information stored on mobile device**
 - None
- **Mobile use deployment**
 - Access via a web browser

The Australian Privacy Principles

Privacy is ingrained into all aspects of our product design and customer engagements. Our data privacy principles, policy and practices are compliant with the Privacy Act 1988 and the Australian privacy principles. This section presents our privacy principles' mapping to the Australian privacy principles, demonstrating our compliance.

I.1 Consideration of personal information privacy

- **APP 1 — Open and transparent management of personal information**
- **APP 2 — Anonymity and pseudonymity**
 - See our privacy principles [A.1 We put a human face to personal data](#) and [A.4 We keep it open, flexible and private](#)

I.2 Collection of personal information

- **APP 3 — Collection of solicited personal information**
- **APP 4 — Dealing with unsolicited personal information**
- **APP 5 — Notification of the collection of personal information**
 - See our privacy principle [A.7 We collect only what is needed](#)
 - We provide conditions for processing personal information to our clients in the service agreements and encourage our clients to do the same for the data they collect and process on our system.

I.3 Dealing with personal information

- **APP 6 — Use or disclosure of personal information**
- **APP 7 — Direct marketing**
- **APP 8 — Cross-border disclosure of personal information**
- **APP 9 — Adoption, use or disclosure of government related identifiers**
 - See our privacy principle [A. 6 We are responsible and compliant](#)

I.4 Integrity of personal information

- **APP 10 — Quality of personal information**
- **APP 11 — Security of personal information**
 - See our privacy principles [A. 2 We think ahead](#), [A.3 We make privacy everyone's business](#) and [A.4 We keep it open, flexible and private](#)
 - We prioritise the confidentiality, integrity and availability of our information assets including personal information. This is reflected in our organisation culture, governance, and business objectives.

I.5 Access to, and correction of, personal information

- **APP 12 — Access to personal information**
- **APP 13 — Correction of personal information**
 - Our clients have unrestricted access to manage their data anytime during their subscription period.
 - See [G.2 Client-managed data export/post-subscription data access](#)