Data Security Policy

Contents

Document Purpose

During the course of our regular business activities, Better Technology Consulting Ltd (hereafter referred to as “us”, “we”, “our” or “BTC) will need to collect, process and store data that has been supplied to us by our clients, in order to undertake the projects that they commission us to do. An example of this would be test data to pre-populate the software solutions that we develop, as well as live data that is generated by the client using our software.

We also generate data internally, including management information, key performance metrics, financial information and internal notes on client projects.

It is imperative that this data is handled appropriately. According to the Data Protection Act 2018 (which is the UK’s implementation of the GDPR regulations), we must ensure that all data held by us is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Thus, the purpose of this document is to outline our data security policy, with regards to all data that is collected, processed and stored by Better Technology Consulting Limited.

Employees and clients can refer to this document to understand the processes that we have in place to adhere to the Data Protect Act and GDPR regulations.

Sources of Data

What data does Better Technology Consulting hold?

The data that we hold can be categorised into one of three main categories: project-related client data, non-project related client data and internal data. Particular care must be taken where we store Personally Identifiable Information (PII) – information which can be used to identify individuals.

Non-project Client Data

Refers to data that is generated and/or collected that pertains to our clients, but does not enter the software solutions that we develop for our clients. Below we have listed some examples of non-project client data, including where it is stored.

- All correspondence between us and our clients are in the format of email communication and phone communication.
- All emails, including attachments, are stored in our Google Mail accounts.
- All other correspondence, including notes based on phone meetings, are stored in the client folder, which is held on our Google Drive.
- Any physical documents are kept in locked pedestals under each employee's desk.

Project Client Data

In order to undertake software development projects for our clients, we will often require them to supply us with data pertaining to the project, e.g. employee details. Depending on the project, the data will end up stored in one of the following locations:

- Excel project files are stored on our Google Drive. This includes both data files sent to us by the client, as well as development files created by us, that may or may not integrate the data sent to us by the client.
- Web application source code is stored in our GitHub repository. This usually does not contain any client data, but sometimes it can, e.g. nomenclature used by the client to describe parts of the system.
- Data that is used by web applications is stored on our dedicated SQL server, within a dedicated SQL server database.

Internal Data

We must apply the same standards of data security to our internal data held at Better Technology Consulting Limited. This is because we store the following data:

- Client contact details for correspondence and billing, which includes names and email addresses, both of which are PII
- Employee details, including names, date of birth, address, employment history and other PII
- Sensitive financial details and strategy documents , which would provide competitors with an advantage if they were to acquire them

Summary

Description	Contents	Security Measures
Google Drive	Client area including correspondence, sensitive documents (e.g. contracts),	Only parts of the drive are available to employees based on permissions set by the MD MD can control access and disable accounts remotely if suspicious access is noticed Drive is cloud-based and regularly backed up
Gmail account	Client correspondence Client files and sensitive documents (attachments)	MD can control access and disable accounts remotely if suspicious access is noticed
GitHub account	Source code for client projects	Connected to Microsoft Account which uses 2FA
SQL Server (on-premises)	Data for client projects, including PII, usernames and passwords (salted and hashed)	SSMS restricted to WeWork office static IP address via Windows Credential set-up on client machines
SQL Azure (cloud)	Data for client projects, including PII, usernames and passwords (salted and hashed)	Portal restricted to WeWork office static IP address Database restricted to either WeWork office static IP or the dedicated IIS webserver static IP
Dedicated server for web application hosting and general file store	Compiled code, and also client uploads which includes PII	Remote Desktop restricted to WeWork office static IP address and TeamViewer only Web Deploy restricted to WeWork office static IP address
Physical	Notes from and about clients and their projects	See Physical Security

Data Retention

Data cannot be stolen, tampered with or otherwise abused if it does not exist. Likewise, incorrect or out-of-date data can result in poor decision making, either by us or our clients. This is why we have a data retention policy, which can help us minimise the amount of confidential data stored by us. The policy applies both to external data supplied to us by our clients, and internal data that is generated as part of our day to day operations.

- Data owners may request a copy of their data and for us to delete their data at any time.
- Data should only be retained as long as necessary. Any data that is no longer relevant to a project should be immediately deleted via a secure method, and care must be taken that shadow copies are not left behind (e.g. Recycle Bin, Google Drive Trash folder)
- Where possible, sensitive data should be anonymised where possible to reduce the impact of a data breach. An example of this would be anonymizing test data for the software that we develop for our clients.

Physical Security

Data is not only stored electronically. It can be stored physically, either in the form of physical media (paper, photographs, sticky notes etc) or electronically on physical devices (hard drives, USB drives, laptops, tablets and mobile phones). It is easy to overlook physical security, especially in a corporate environment, therefore we have the following policy in place to mitigate the risk of a breach:

- All employees should use their keycard to access the Better Technology Consulting Ltd office in Aldgate Tower. If your keycard has gone missing, inform the MD immediately, who will liaise with WeWork to cancel your old card and issue you with a new one.
- When entering the floor that the office is on, care must be taken as tailgaters can enter. Suspicious visitors should be reported to reception who will contact security.
- Computers and all other electronic devices (e.g. phones, tablets and laptops) should be “locked” when the employee are not present; thus if an unauthorized person manages to physically access the office, they will be unable to access any of our devices that contain sensitive data.
- Each employee has a pedestal with a non-lockable and a lockable section; the lockable section should be used to store any sensitive physical documents; again this adds a layer of protection if the office is breached by an unauthorised person.
- The office is lockable and each employee has a key, which should be used to lock the office if no other employees are present.

Portable Devices

- Should always remain in the head office when not in use.
- Follow the office physical security policy around ensuring the office is locked when no employees are present, and challenging any unauthorised visitors to avoid theft.

- Notify the MD and update the physical device log with the date/time of signing it out, the employee that has signed it out, and (upon return) the date/time of signing it back in.
- Ensure that when out in public places, employees maintain visual contact with portable devices at all times. Care must be taken in busy places such as coffee shops, pubs, and train stations.
- If a device is suspected to be missing, notify the MD immediately, and inform the nearest authorities as required. For example, if a company laptop is lost in a pub, after contacting the MD, liaise with the pub manager to determine whether anyone has sighted the lost/stolen property, and may be able to assist with looking at CCTV. Inform the police if a crime is suspected.
- The MD will be responsible for contacting the ICO and all clients who may be affected by the loss of physical property.

Data Transmission

This section outlines the standard procedures that should be undertaken when transmitting data both internally and externally.

Transmission of data

- Gmail is secured using SSL which prevents man-in-the-middle attacks as all data is encrypted prior to transmission.
- Large file transfers are performed using a direct link via Google Drive which is securely connected to the BTC machine via Gmail account or WeTransfer, where files are encrypted when they are being transferred (TLS) and when they are stored (AES-256). Once your files are safely stored, they can only be accessed using the unique links sent to the sender and recipient.
- No other medium of transfer is used (e.g. floppy disk, USB stick, CD-ROM)
- All connections to our dedicated server (excluding port 80, for HTTP and 443 for HTTPS) are IP address restricted via a static IP VPN service.

Sharing of data

- Any Google Drive folders that are accessible to our clients is strictly access controlled via a pre-shared link, sent via email directly to the client in question.
- These folders only contain information relevant to the client that it relates to and are regularly purged of non-essential data.

Hardware and Software Configuration

Data security can be improved via the correct configuration of the hardware and the software that it is stored on. Since hackers are always attempting to find new vulnerabilities in the hardware and software that we use, it is important that we are always keeping our hardware and software up-to-date with the latest patches and configured correctly.

It is forbidden for employees to tamper with the default configuration without express permission from the MD.

Patching

All of our desktop and laptops run Windows 10 as their operating system, and are set to automatically download and install the latest patches in the background.

The dedicated server runs Windows Server 2012 and is set to automatically download and install patches every weekend. Critical updates may require a manually update and restart during non-office hours (usually after 9pm).

Anti-virus/anti-malware (AV/AM)

All computers have the latest anti-malware software installed, which is regularly updated on an automatic schedule via background updates, provided the computer is connected to the internet.

Virus scans are performed in the background on a daily basis.

If the AV/AM software flags a threat, it will be quarantined. However, the MD should be informed straight away, and will advise if any further actions are required. Further actions may include investigating the source of the threat, and notifying third parties that their systems might be compromised.

IP address restrictions

The dedicated server has the remote access and SQL server ports restricted to the static IP of the Better Technology Consulting Ltd office.

TeamViewer can be used to securely log in to the server if employees are working remotely.

Firewall

The firewall should be regularly reviewed to ensure that only necessary ports are open on our web server.

Logging

Going through logs is usually the first step taken when attempting to identify a potential cyber-attack. Therefore it is essential that our logs are configured correctly and retained for long enough to provide us with enough information on what actions have occurred, in order for us to respond to the threat in the most effective manner.

We store logs on both our dedicated server, and our Azure apps use Advanced Threat Monitoring to proactively advise us of potential weak spots and unusual activity.

Dedicated server logs can be viewed using Event Viewer, and SQL Server Agent. The combination of both allows us to look for failed logon attempts on either the web server itself (via Remote Desktop) or directly connecting to the SQL database (in the case of Azure databases)

Logs should be retained for a minimum of 180 days. The most critical logs that should be reviewed on a regular basis are listed below:

- Dedicated server: Windows event viewer log
- Dedicated server: Application event viewer log
- Dedicated server: SQL server event log
- SendGrid: email activity log
- Azure portal: activity log

Passwords

Most of the systems that we use are secured using a username/password combination. Given that the username is static, it stands to reason that a strong password is the only effective defence against a hacker using a password guessing attack vector.

A common error is to use a single complex password for all systems, however this means that once the password is compromised, all systems are compromised. This is why we use a password manager to allow us to easily generate and store unique passwords for each system. The password manager requires a key which can only be accessed via the Google Drive, and the Google Drive is secured via a central administrative console and also uses two-factor authentication.

Our password policy is as follows:

- KeePass 2.0 is used as the standard password manager within the company, which has a secure database for the common passwords required by all employees and requires a composite master key for access.

- Access to the password manager is provided by the Managing Director, administered via the secure master key file. Control to this key file is via a physical USB device and the MD can change the master key at any point by re-issuing new USB devices in the case of a physical breach.
- KeePass 2.0 should be used to generate very strong passwords and remember the password for you. It will automatically set an expiry date on the password.
- A longer password is more secure than a complex one – aim to generate passwords of at least 16 characters, however for business-critical systems we use passwords of up to 64 characters. KeePass 2.0 can generate strong passwords of any length, and should be used to avoid creating easily-guessed passwords.
- Once a password is nearing expiry, ensure that you change it to a new one within the relevant system and update the entry in the password manager.
- Do not reuse passwords. If a password is compromised, hackers might attempt to enter other systems using the compromised password. By not reusing passwords we can mitigate this risk.
- Passwords must never be stored or written down anywhere, other than securely within the KeePass 2.0 password manager.

Software Development Principles

Our cloud-based software solutions are public-facing and can allow any user to attempt to log in. Whilst this is a bonus for our clients who require access to their system from any location, it allows hackers to attempt to log in as well, therefore we must be extremely careful with how we design our software to mitigate against this. This is done in the following way:

- Use of ASP.NET identity, an industry-standard framework, developed and maintained by Microsoft, for allowing users to securely log in using a username and password, as well as manage user accounts.
- Parameterised queries and avoidance of dynamic SQL, to prevent SQL injection attacks. All new web applications use Entity Framework (EF6 for .NET Framework and EFCore for .NET Core) as an ORM, which automatically generates safe SQL statements from C# code.
- Use of anti-forgery tokens to prevent cross-site scripting attacks.
- Custom error pages to prevent useful information being leaked to hackers.
- Regular penetration testing by external agencies to determine vulnerabilities .

- All passwords stored in SQL databases are salted and hashed using a secure algorithm. Identity uses PBKDF2 with HMAC-SHA1, 128-bit salt, 256-bit subkey, 1000 iterations.

Example of Threats and Mitigations

The threat landscape consists of internal threats and externals threats. Threats can also be malicious (in the case of deliberate breach of our data security protocols) or accidental.

We have listed some examples of the different type of threats below in order for you to be aware of varying nature of these threats, however this is not an exhaustive list and we urge vigilance whenever dealing with data.

External threats

Hackers (external agents operating outside of Better Technology Consulting who are trying to access, copy, steal, modify or otherwise interfere with data held by us, might use some of the following method to breach our data security defences, via some of the following methods:

- Password guessing. Mitigation: strong passwords, following our internal password policy, changed regularly, not easily guessed, with minimum length and special character requirements. Highly sensitive systems use two-factor authentication where possible. IP address restrictions to prevent users outside our network from being able to attempt to log in to critical infrastructure.

- Man-in-the-middle attacks. Mitigation: only connect to secure, approved WiFi networks. Do not use free WiFi hotspots, cellular data is preferred in this situation and data costs will be reimbursed by the company. Always ensure HTTPS in enabled on all sites, and disallow non-HTTPS communication with websites.

- Social engineering. Hackers can use publicly available information on social media to pose as familiar people and request information from employees that can be used to undermine our defenses. Mitigation: employee training to recognise the telltale signs of a social engineering attack. Policy to escalate any suspicious calls to the MD if in doubt. Employees advised to limit personal information on social media where at all possible.

- SQL injection attacks. As most of our data for our client projects is held within SQL databases, hackers might potentially try to use SQL injection attacks to hack our databases. Mitigation: use parameterised queries and avoid dynamic SQL statements. Any and all dynamic SQL must have the approval of the MD and should only be used if completely unavoidable. Use of our ORM (Entity Framework) where possible.

- Cross-site scripting attacks. Hackers might attempt to use cross-site scripts to execute JavaScript code on our web applications which might be malicious. Mitigation: policy

to disable cross-site scripting via the anti-forgery token which is set a default as part of the Microsoft Identity framework.

Internal threats

- We trust our employees to undertake their duties in a responsible manner, and as part of that trust, some employees are privy to sensitive client data or possess passwords that are used to access critical systems.
- Sadly, history has shown us that some companies can be vulnerable to internal attacks from disgruntled or otherwise hostile employees. Therefore it is important to limit access to sensitive data to only those employees who require it, and forbid the sharing of passwords or other credentials.
- The central GSuite administration console allows users to have their accounts disabled remotely in case rogue behaviour is detected.
- Employees are contractually obliged to adhere to this Data Security policy and any breaches may result in disciplinary action, up to and including gross dismissal.
- Our password security policy states that passwords should be rotated on a regular basis, and also as soon as an employee leaves, to mitigate against unauthorised users from being able to access protected systems
- Logs should be reviewed on a regular basis in order to identify suspicious patterns of behaviour, such as logons outside of working hours.

Non-malicious threats

- Clients or employees might accidentally forward sensitive information to other users. Therefore it is imperative to avoid attaching information in emails and prefer the sending of files via a direct link to our Google Drive, as well as attach a disclaimer to all emails warning clients to treat sensitive information with care.
- If attachments must be used and it contains PII, ensure that the attachments are password protected and the password is sent in a separate email. If the accidentally forwards the email to an unauthorized party, the unauthorized party will not be able to view the data without the password.
- Physical data (such as data stored on a USB key or on company laptops) might get lost or stolen. Employees must adhere to the portable devices policy, and also to password protect USB drives and company laptops with strong passwords.

Handling a Data Breach

According to the ICO's website:

"The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify."

In the unfortunate event of a data breach, the procedure is as follows:

- Inform the MD immediately. The MD can then allocate additional resources to assist and will act as your point of contact to assist you with handling the breach.
- Secure the affected system(s) as soon as possible. This may include shutting down the dedicated server, stopping Azure instances, or deactivating user accounts via the GSuite console.
- Notify any clients that will be affected by the shutting down of any of the services, and let them know that a critical incident has occurred, that we are investigating and will contact them with an update within 24 hours.
- Assist the MD and any other resources with investigating and tracing the source of the breach.
- Begin securing any other systems that are live but might be affected, e.g. if the password database is compromised new passwords will need to be generated and set on all relevant systems.
- Begin securing the system that has been compromised; if it is one of our software products, a code review will need to take place.
- Within 72 hours the MD will contact the ICO and all affected clients to inform them of details of the breach if required.
- Once the breach has been secured, an investigation will commence to identify how the breach occurred, what were the weak points and what lessons can be learnt in order to implement more effective controls in the future. The investigation and results of the investigation will be made available to the ICO and our clients.

Although we hope this event remains a theoretical possibility, it is important to be prepared in case it happens, so we can act swiftly and effectively to minimise damage to ourselves and our

clients. The most important thing is to be honest and not panic; the priority here is not to blame others but to secure our systems and repair any damage done.

Policy last reviewed:

By: 

Name: Lee Ramsingh

Title: Managing Director

Date: 25/06/2020