# IT Security Policy

| | |
|---|---|
| Document Type | Policy |
| Document owner | Jonas Bruun Jacobsen, Chief Technology Officer, BeCause ApS |
| Approved by | Management Board |
| Approval date | January 2024 |
| Review date | January 2024 |
| Version | 2.1 |
| Amendments | January 2024 |
| Related to | - |

*Do you have a formal Security Incident Management Process in Place?*

## 1 Introduction

BeCause ApS (the “Company”) offers companies a completely different approach to their sustainability information management infrastructure. Instead of collecting, coordinating, and communicating sustainability information via a complex, fragmented and manual stack of files, mails, and niche-purposed systems, we're a unified single source of truth and automated data hub for our customers, taking away 100% of the pain of management fragmentation. It's faster, safer, simpler, and above all, way better.

This IT Security policy applies across our application-, infrastructure- and HR resources, and displays what actions we are taking to ensure the confidentiality, integrity and available of our services.To readers not employed by BeCause, we encourage reading this IT Security Policy fully first and then recommend any feedback. To BeCause employees, we always expect BeCause employees to act in full compliance with all policies contained herein. Security is everyone’s responsibility at BeCause.

We value any feedback to this policy. Please forward any such feedback to privacy@because.eco.

### 1.1 Scope

This policy applies to all staff, contractors, students and interns at BeCause ApS.

## 2. Policies

### 2.1 Application Security Policy

At Because we shape the development culture from the start into producing more secure code. All BeCause developers follow and have read the OWASP Top 10 Critical Security Risks guidelines, before they start coding. Furthermore, each year we host an internal security workshop, where also the OWASP Top 10 for the new year is presented.

For all systems developed by BeCause, we enforce good-practice password policies, such as minimum password lengths and the option of 2FA to the users.

We finally have a Vulnerability Disclosure Policy in place for issues found by external parties.

### 2.2 Infrastructure security

Test, Staging and Production Environments:
The Because Test, Staging and Production environments are physically separated and lives as completely different applications. The users and logins are as a result also fully separated for the environments, and any data that may be copied from production to the Staging or Test environment (e.g., for troubleshooting purposes) are first anonymized such as to no longer contain any sensitive, identifying or contact information-related data.

IP whitelisting:
The set of IPs that can access the underlying resources in Microsoft Azure (such as databases) are limited to only the office IPs, or the IPs of individual BeCause developers that needs remote-working capabilities. The whitelisting of individual developer IPs are on a need-to basis and needs to be requested to the CTO of BeCause.

DDOS protection:
BeCause uses Cloudflare as DNS provider. As part of Cloudflare's offerings, we are protected through them should the event happen that we become target of DDOS attacks.

### 2.3 People Security

The employees of BeCause are only given access to data on a need-to basis, and never to more than needed, nor with higher access rights than needed (e.g. a data analyst only has read-access to data and only to the relevant data). When employees leave the company, they are off boarded from all systems, and requested (pr. their mandatory NDA with BeCause) to hand over any sensitive information related to the nature of BeCause or their clients.

Any employee at BeCause are trained in what phishing is, and they are required to use 2FA for all services they use related to BeCause and are prohibited from sharing these accesses. Furthermore, at BeCause we focus on having role redundancy, such that in the event something happens to one employee, they were not the sole employee with access to any systems.

The list of BeCause employees that have elevated access (i.e. "superusers") to any feature on the BeCause platform itself is curated and controlled by the CTO.

Any BeCause employee, regardless of their role or access rights at BeCause, is to leave their IT equipment in a secure state (e.g. never showing sensitive data and on lock screen), whenever they are not close to it.

Finally, all BeCause employees are to read this policy as part of their onboarding process and are notified of any changes that affect them.

### 2.4 Data Backup & Data Retention

SQL Databases:
Backups are made every month of every SQL database at BeCause. Each day in between the full backups, we are creating differential backups. Finally, we support PITR (point-in-time restore) on our databases for any point within the last 7 days. Backups are kept for 60 days, after which they are automatically destroyed.

Blob storage:
Non-critical data such as response payloads to API requests are logged and stored in Azure Blob storage. All blob storage containers are running with a 30-day soft delete policy before any data-deletion becomes permanent.

Codebase:
All written code for any system or service that constitutes a part of the BeCause platform infrastructure is under version control. This means that all changes to any part of the codebase are versioned and rolling back to earlier codebases are possible. There is no expiration here and all old code-versions are kept.

We perform backup recovery tests regularly.

### 2.5 Sensitive information Policy

All data received from platform users and integrating data providers needs to be classified into sensitive, personal or non-personal data. Any password-related information is not to be sent to, stored nor logged on any BeCause system, and is instead to be handed by our third-party authentication provider, Google Firebase.

All information should be safeguarded according to its sensitivity, and sensitive or personal data is only to be copied or transmitted – whether over removable media or the internet - when the confidentiality of the data can be assured, and there are no realistic alternative ways of achieving a similarly satisfactory result without transfering of the data in question.

Any access related information (passwords, tokens, symmetric keys, private keys and similar) are always considered sensitive information. Personal identifiable information are similarly always considered sensitive. For other types of data, the employee must on a pr. case basis exercise the appropriate judgement in whether a piece of information is sensitive, and if in doubt contact the data protection officer of BeCause ApS.

### 2.6 Data incident & Informing Stakeholders

BeCause defines a data incident as any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of the users of BeCause.

In the case of a data incident, BeCause will contact the companies whose personal data is affected. If the data was provided by a data provider integrating with BeCause, the data provider will be informed without any undue delay. The notice will contain at the least:

- The number of data subjects concerned, date and time of the incident, summary of the incident that caused the personal data breach, and the nature and the content of the personal data concerned.
- The circumstances of the personal data breach (e.g. loss, theft, copying).
- The identity and contact details of Because's data protection officer or other contact point where more information can be obtained.
- Recommend measures to mitigate the possible adverse effects of the personal data breach.
- Describe the likely consequences and potential risk to the data subject due to the personal data breach.
- Describe the measures proposed or already taken by BeCause and its employees to address the personal data breach.

Any data incidents should be reported without undue delay to privacy@because.eco and the CTO of BeCause (jonas@because.eco).

### 2.7 Business Continuity & Disaster Recovery

Business continuity during physical incidents:
Our overall approach to business continuity involves ensuring that all our systems are Software as a Service ("SaaS"), so in the event of a **disaster at the BeCause offices**, all BeCause employees can work remotely and our services stay available for the customers. In the unlikely event that the **Microsoft Azure data center has an incident**, Cloudflare provides an extra layer of caching on top of our own, securing often accessed data available for another 2 hours, while the data center is being resolved.

Business continuity during application and infrastructure incidents:
Our platform is designed to follow the micro services pattern to secure high uptime. Even if an feature/service on the platform goes down, the other features stays available while the individual micro service issue is resolved. Furthermore, the widget- and integration micro services that hosts the APIs that any integrating partner-systems integrate with, has their own local copies of the relevant BeCause data and runs on their own dedicated hardware, such that they can keep serving clients, even if all other services are down.

Finally, a snapshot is made of all software-versions rolled out, which allows us to quickly roll back the software running on any micro-service to an earlier version that worked, if a deployment of new code fails. If a software rollout fails and has an impact on the databases and/or data they contain, we are also able to roll back the databases to the point in time prior to the software rollout. See our data backup policy for more info here.

Business continuity during people incidents:
Should disaster befall a BeCause employee, there will always be a role redundancy between people. No single person has the sole knowledge or access to something that is needed to keep BeCause running. For the platform

access keys and infrastructure setup, the access is shared between the CTO and Head of Development at BeCause.

See the separate Disaster Recovery Policy for the detailed disaster recovery response.

### 2.8 Monitoring and Logging Policies, Standards, and Procedures

Regular logging and logging availability:
All logins, performed actions and data requests by BeCause employees, integrating partner-systems and users are logged by BeCause for a minimum of 30 days, and for an extended period in situations deemed critical, such as audit logs for when access to a company's data has been requested.

Whenever the logs are relevant for customers, such as audit logs for when other companies' (that has been granted access) views a company's data, the log is also made available to the company itself through the BeCause platform.

No sensitive information such as passwords or similar shall ever be logged.

Application and system logs:
All exception issues (bugs) occurring on BeCause, as well as regular API requests and application flows (traces) are logged by BeCause, and the lists are continuously monitored by BeCause to secure a high quality of the BeCause platform.

### 2.9 Encryption standards and key management.

All data at rest within BeCause's platform are hosted on Microsoft Azure SQL Servers and are encrypted following the standards of their Transparent data encryption solution. At this point (Q2, 2022), this means all data in the SQL databases, the backups and the logs are encrypted with AES 256 encryption and encrypted/decrypted in real-time as needed.

All keys are stored in Azure Key Vaults (with access given to the CTO and Head of Development), and key rotation is performed at least every 6 months.

Finally, all access to third party services for which BeCause employees need to keep track of login-credentials, these credentials are to be stored in a password-manager application approved by BeCause.

## 3. Compliance with Applicable Laws and Regulations for the Protection of Personally Identifiable Information

BeCause ApS is committed to complying with all applicable laws, rules and regulations related to the protection of personally identifiable information. The Company will take all necessary steps to ensure that its personnel and contractors receive appropriate training and are subject to appropriate contractual conditions, to ensure their actions comply with applicable laws and regulations. Any inqueries into BeCause ApS's compliance with the law needs to be directed to BeCause's Data Protection Officer.

## 4. Contact Information

If you have any questions regarding our IT Security Policy, please find our contact details below:

BeCause ApS
Njalsgade 21 E, 1
2300 Copenhagen S, Denmark
Corporate Identity Number: 39745267
Email address: privacy@because.eco.

And for any direct contact, please contact BeCause's Data Protection Officer:

Jonas Bruun Jacobsen,
CTO & Chief Privacy Officer, BeCause ApS,
Email address: jonas@because.eco