YOURWELLSPACE LTD
11 Dormer Place
Leamington Spa, UK
CV32 9AA

Wellspace ICT Security Statement

LAST UPDATED: JULY 2022

AUTHOR

Paul Henderson - C.T.O

INDEX

GDPR PRIVACY POLICY

Overview

The General Data Protection Regulation (GDPR) is the most significant legislative change in European data protection laws since the EU Data Protection Directive (Directive 95/46/EC), introduced in 1995. The GDPR became enforceable on May 25, 2018, strengthens the security and protection of personal data in the EU and serves as a single piece of legislation for all of the EU. It replaced the EU Data Protection Directive and all the local laws relating to it.

Wellspace supports the GDPR and all of our services comply with its provisions. Not only is the GDPR an important step in protecting the fundamental right of privacy for European citizens, it has raised the bar for data protection, security and compliance in the industry.

Wellspace is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data and Wellspace will comply with applicable GDPR regulations including as a data processor, while also working closely with our customers and partners to meet contractual obligations for our procedures, products and services. Our team of experienced business analysts, consultants and digital specialists will also help to support customers in meeting their obligations through the provision of expert services and value-adding solutions.

Contact Details

The Data Protection Officer

Yourwellspace Ltd

11 Dormer Place

Leamington Spa - UK

CV32 5AA

info@yourwellspace.com

Wellspace as a Data Controller

Under current GDPR definitions, Wellspace act's as both a Data Controller and a Data Processor due to the analytical nature of our service, we are given data by a "Controller" and as such Wellspace acts as a "Processor". In the course of delivering business objectives, data is analysed and used to generate reports and form suggestions that have an impact on the end users we support, in this respect, Wellspace act's as a Data Controller.

In the course of its daily organisational activities, Wellspace acquires, processes and stores personal data in relation to:

- Employees of Wellspace
- Customers of Wellspace
- Third party service providers engaged by Wellspace

In accordance with GDPR legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in GDPR legislation. However, Wellspace is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a GDPR issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Wellspace, there is regular and active exchange of personal data between Wellspace and its Data Subjects. In addition, Wellspace exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with Wellspace's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Wellspace staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Collection and Use of Personal Information

To enable us to provide quality services to you, we need to collect anonymous and Personal Information about you. "Personal Information" means any information concerning the personal or

material circumstances of an identified or identifiable individual. We collect Personal Information through your use of the Software and related services such as the Wellspace Smartphone Applications, Information you provide related to your use of the website and mobile applications (e.g. through the use of cookies).

Your Personal Information includes, but is not limited to, your:

contact Information, such as your name, address, email address, phone number provided by your employer, or which you provide when you enrol as a user of the service, upload or submit activity information or any material via the website or request any information; email address in connection with your account sign-in facility;

gender and age when you enrol and in connection with your account profile;

information collected through the use of our software and related services about your health, fitness and related activities including technical information from your fitness device; record of your participation in activities and challenges and your rewards;

information you post in the form of comments or contributions to discussions, and communications you send us to submit queries or comments regarding the website or its content.

You are under no obligation to provide any Personal Information to us at any time. However, if you should choose to withhold specific information, we may be unable to provide you with certain services.

We will use your Personal Information only for the purpose of providing our services to you, including to: Administer your account with us; Identify you when you sign in; Track your programme progress and determine your eligibility for rewards, as well as provide you with information that you may find helpful; Analyse on an anonymous, aggregated data basis the use of the website and the people visiting in order to improve our content and services, including research into our users' demographics; and send you information that you have requested from us.

Push Notifications

We send you push notifications on your device from time to time in order to provide you with in-product reminders and notifications. If you no longer wish to receive these types of communications, you may turn them off at the device level.

Informational Emails

Wellspace may send you emails or newsletters with information and offers about the Wellspace platform and services. You can opt out of such communications free of charge at any time by sending an email to info@yourwellspace.com

Additional Information

When you visit the website we may automatically collect additional information such as the type of Internet browser or mobile device you use, your IP address (the unique address that identifies your device on the internet) and the operating system of your device, which is automatically recognised by our web server. We use this information to derive a broad, non- specific understanding of the locations from which you are accessing our services, to analyse trends, administer the site, track users' movements around the site and to gather demographic information about our user base as a whole and to personalise the website to users' preferences.

Information Sharing

In general, we will use and disclose your Personal Information to administer our services to you including, at times, disclosing your Personal Information to agents or contractors that work on our behalf and assist us in providing and supporting the services we offer through the website including processing transactions, fulfilling requests, analysing data or helping us to communicate with our members. We may also disclose your Personal Information if you have expressly consented to this

In addition, we may use your Personal Information, in connection with your participation in our services and your possible participation in other third-party-provided wellness services ("Third-Party Providers") that may be offered to you by us, your employer or entities with which your employer contracts, for the following general purposes:

to coordinate (x) enrolment in, (y) enhancement of your experience and (z) education about the services available to you through our platform such as a Wellbeing Appraisal Report or any related wellness services provided by a Third-Party Provider,to ensure that you receive appropriate rewards for participation in our services and other similar services provided by your employer or entities that contract with your employer,to evaluate the overall quality and effectiveness of the programme(s) in which you may participate; and to assess your eligibility for other programmes that your employer or contractors on behalf of your employer, may offer.

To the extent you participate in any wellness challenges or competitions that we sponsor, please be aware that your name and performance information will be available to other wellness challenges or competition participants and to your employer if you opt in to make your data visible.

Except as described in this Privacy Policy, we will not sell, rent or make available your Personal Information to third parties without your permission. Unless in using the website or mobile applications you expressly or impliedly agree to make certain information available, all Personal Information that we collect is kept confidential to the best of our ability, subject to the other terms and conditions of this Privacy Policy. In addition, our employees and contractors who provide services related to our website or mobile applications are obliged to respect the confidentiality of any Personal Information held by us. Our employed staff and contractors are authorised to use your Personal Information only as necessary to provide these services to us.

In the event that we undergo re-organisation or are sold to a third party, any Personal Information we hold about you may be transferred to that re-organised entity or third party in accordance with applicable law. You acknowledge that such acquisitions may occur, and that any acquirer of Wellspace or its assets may continue to use your Personal Information as set forth in this Privacy Policy.

Wellspace may disclose your Personal Information (a) if legally entitled or required to do so (for example if required by law or by a court order or other judicial or administrative proceeding, (b) as otherwise required under any applicable law, rule or regulation and (c) if we believe, in good faith, that such disclosure is necessary to protect or defend our rights or those of others or to assist in the investigation or prevention of illegal activity.

The website may use message boards and messaging forums that will be available to its members. Any information that is disclosed in these areas may become public information and you should exercise caution when using these and disclosing your Personal Information.

Access upon request we will provide you with information about whether we hold any of your Personal Information. If your Personal Information changes or is incorrect or outdated, you may correct, update or amend it by making the change through the “my account” section of the website. If you no longer desire our service, please contact info@yourwellspace.com to discuss cancelation.

Anonymous Information

We may create “Anonymous Information” records from the Personal Information records by excluding your Contact Information or excluding any other information that could link the

Anonymous Information back to you. We may use this Anonymous Information for internal purposes, such as analysing patterns in the programme usage, so that we may enhance the services. We reserve the right, subject to applicable law, to use and disclose any Anonymous Information at our discretion. For example, upon request by your employer, we may share Anonymous Information with other partnering organisations for purposes of research and programme analysis. You are welcome to request the names of such partnering organisations from us at any time. We use this Anonymous Information to analyse and understand demographics trends, customer behaviour patterns and desires, and information that may enrich the content and quality of our member programmes.

If you are a member of the Wellspace service we may (a) share Anonymous Information with your employer in an anonymous aggregated or group format and (b) provide your Personal Information in an anonymous aggregated or group format to third parties ("Analytics Processors") that process that Personal Information to generate Anonymous Information and analytical information related to that Anonymous Information to be shared with your employer. Your employer will not be able to use such Anonymous Information to directly identify you. Your employer may use this Anonymous Information in its discretion, including to evaluate the programme overall as well as to provide additional benefits, programmes and services.

The Analytics Processors do not have any independent right to use your Personal Information except to provide services to generate the Anonymous Information and analyse the information to generate general analytical information. You are welcome to request the names of such Analytics Processors from us at any time.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems. Any data that you download to your own systems should be held securely with restricted access.

Customer Data Retention

Customer accounts are soft deleted upon request, data is retained for 90 days should the user wish to re-activate their account. After 90 days all data is deleted from the platform.

PASSWORDS

Password Encryption

Passwords are stored and hashed using Bcrypt, Bcrypt is a great choice for hashing passwords because its "work factor" is adjustable, which means that the time it takes to generate a hash can be increased as hardware power increases.

BCrypt is based on the Blowfish block cipher cryptomatic algorithm and takes the form of an adaptive hash function. Using a Key Factor, BCrypt is able to adjust the cost of hashing. With Key Factor changes, the hash output can be influenced. In this way, BCrypt remains extremely resistant to hacks, especially a type of password cracking called rainbow table.

Portal

- Minimum 8 Characters
- At Least 1 UpperCase
- At Least 1 Number
- At Least 1 Special Character

Application (iOS/Android)

- Minimum 8 Characters
- At Least 1 UpperCase
- At Least 1 Number
- At Least 1 Special Character

PHYSICAL DATA SECURITY

Physical Security

Wellspace utilises hosted virtual private servers provided by DigitalOcean, hosted in Tier 4 data centers which are co-located in some of the most respected data center facility providers in the

world. As such, all data centres guarantee a 99.995% availability. We leverage all of the capabilities of these providers including physical security and environmental controls to secure our infrastructure from physical threat or impact. Each site is staffed 24/7/365 with on-site physical security to protect against unauthorized entry. Security controls provided by our data center facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located data center within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

Infrastructure Security

Our infrastructure is secured through a defense-in-depth layered approach. Access to the management network infrastructure is provided through multi-factor authentication points which restrict network-level access to infrastructure based on job function utilizing the principle of least privilege. All access to the ingress points are closely monitored, and are subject to stringent change control mechanisms.

Systems are protected through key-based authentication and access is limited by Role-Based Access Control (RBAC). RBAC ensures that only the users who require access to a system are able to login and also can only access data relevant to their role. We consider any system which houses customer data that we collect, or systems which house the data customers store with us to be of the highest sensitivity. As such, access to these systems is extremely limited and closely

monitored. Additionally, hard drives and infrastructure are securely erased before being decommissioned or reused to ensure that your data remains secure.

Access Logging

Systems controlling the management network at DigitalOcean log to our centralized logging environment to allow for performance and security monitoring. Our logging includes system actions as well as the logins and commands issued by our system administrators.

Security Monitoring

Our Security team utilizes monitoring and analytics capabilities to identify potentially malicious activity within our infrastructure. User and system behaviors are monitored for suspicious activity, and investigations are performed following our incident reporting and response procedures.

Server Security & Employee Access

The security and data integrity of our data is of the utmost importance at our data centre. As a result, technical support staff do not have access to the backend hypervisors where virtual servers reside nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only select engineering teams have direct access to the backend hypervisors based on their role.

Snapshot and Backup Security

Snapshots and Backups are stored on an internal non-publicly visible network on NAS/SAN servers. We can directly manage the regions where our snapshots and backups exist which allows us to control where our data resides within our data centers for security and compliance purposes. Data is never held on physical mediums such as CD/DVD/USB, staff are required to ensure that data downloaded to laptops/desktops for purposes of analysis is deleted upon completion of the required activity.

APPLICATION DATA SECURITY

OAuth 2

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean. It works by

delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices. The application is further secured by utilising AES256 encryption.

SUPPLIER COMPLIANCE

Data Centre Standards

- ISO/IEC 27001:2013 - LINK
- SOC1 Type II - LINK
- SOC2 Type II - LINK
- PCI DSS - LINK

Web Performance & Security

Wellspace currently utilises Cloudflare for web performance and security and conforms to:

- ISO/IEC 27001:2013
- SOC2 Type II
- SOC3
- PCI DSS 3.2.1
- 1.1.1.1 Public DNS Resolver Privacy Examination

DATA TRANSFER POLICY

Overview

The European Union (EU) Data Protection Directive 2016/680 of the European Council of 27 April 2016 (the "Directive") applies to all Member States of the EU. Special precautions need to be taken when personal data is transferred to countries outside of the European Economic Area ("EEA"), i.e. in case of transfers to countries such as the United States, which do not provide EU-standard data protection.

About the Model Contract Clauses

The EU Commission has published model contract clauses for data transfers (the "Model Contract Clauses") and determined that organizations which use the Model Contract Clauses offer sufficient safeguards for cross-border data transfer as required by the Directive. Accordingly, each Wellspace Entity shall enter into a set of Model Contract Clauses with the respective Wellspace entity receiving Personal Information from the EU. Two sets of standard contractual clauses have been adopted for transfers between Data Controllers,and one set exists for transfers between a Data Controller and a Data Processor. Which set of Model Contract Clauses to use depends upon whether the company receiving the data is a Data Controller or a Data Processor. Further, whether a company is a Data Controller depends upon whether that company determines how the data is processed.

Scope

This Policy governs Personal Information (as defined below) received from the entities about i) employees (potential, current or former), contractors and contingent workers; ii) business entities and individuals referenced in contractual documentation and retained in Wellspace's centralized electronic repository of executed agreements; and iii) individuals processed within certain information technology applications or platforms that support our business functions and which are hosted, supported or maintained by Wellspace. Personal information that is transferred from the entities to Wellspace is used to carry out and support human resources, contract management,information technology provisioning and related activities.

Definitions

"Wellspace" means Yourwellspace Ltd.

"Controller" means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or European Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or European Community law.

"Personal Information" means any information that identifies or could be used to identify an individual. Personal Information does not include information that is anonymized so as not to permit identification of the relevant individual. Notwithstanding the above, to the extent such information is deemed personal information or personal data in an EU member state,Wellspace will treat such information as Personal Information under this Policy.

"Processing" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,alignment or combination,blocking,erasure or destruction.

"Processor" means the natural or legal person, public authority, agency or other body which processes personal data only on behalf of the Controller and as instructed by the Controller.

"Sensitive Personal Information" means personal information about an individual's race, ethnic origin, political opinions,religious or philosophical beliefs,trade union membership, sexual orientation, physical or mental health condition, and data relating to offenses, and/or criminal convictions. In addition, Wellspace shall treat as Sensitive Personal Information any information received from a third party where that third party determines that information to be sensitive and Wellspace agrees with this determination in writing.

Privacy Principles

Model Contract Clauses' Principles: Wellspace will comply with the principles set out in the applicable set of Model Contract Clauses (Controller to Controller, or Controller to Processor clauses).

NOTICE: The respective transferring Wellspace entity will,as required by law,inform individuals about the purposes for which it collects and uses Personal Information, how to contact such Wellspace entities, the types of third parties (including other Wellspace entities) with which it shares that information. If a Wellspace entity transfers data to Wellspace,it will also inform the individual about this transfer, the purposes of the transfer and how the receiving entity can be contacted. This information will be provided as soon as practicable and, in any event, before Wellspace uses the information for a purpose other than that for which it was originally obtained.

Wellspace may not need to furnish notice where providing notice is not required by law, in cases where, subject to applicable EU data protection laws, the Processing in question is necessary to respond to a government inquiry;is required by applicable laws, court orders or government regulations; in the case of a merger or acquisition,or is necessary to protect Wellspace's legal interests (each to the extent allowed under applicable EU data protection laws).

Data Integrity

Wellspace seeks to ensure that any Personal Information held about individuals is accurate,complete,current and otherwise reliable in relation to the purposes for which the information was obtained. Wellspace seeks to collect PersonalInformation that is adequate, relevant and not excessive for the purposes for which it is to be processed. Wellspace employees have a responsibility to assist Wellspace in maintaining accurate, complete and current Personal Information.

Transfers to Agents or 3rd Parties

In general, we will use and disclose your Personal Information to administer our services to you including, at times, disclosing your Personal Information to agents or contractors that work on our behalf and assist us in providing and supporting the services we offer through the website including processing transactions, fulfilling requests, analysing data or helping us to communicate with our members. We may also disclose your Personal Information if you have expressly consented to this

In addition, we may use your Personal Information, in connection with your participation in our services and your possible participation in other third-party-provided wellness services (“Third-Party Providers”) that may be offered to you by us, your employer or entities with which your employer contracts, for the following general purposes:

to coordinate (x) enrolment in, (y) enhancement of your experience and (z) education about the services available to you through our platform such as a Wellbeing Appraisal Report or any related wellness services provided by a Third-Party Provider,to ensure that you receive appropriate rewards for participation in our services and other similar services provided by your employer or entities that contract with your employer,to evaluate the overall quality and effectiveness of the programme(s) in which you may participate; and to assess your eligibility for other programmes that your employer or contractors on behalf of your employer, may offer.

To the extent you participate in any wellness challenges or competitions that we sponsor, please be aware that your name and performance information will be available to other wellness challenges or competition participants and to your employer if you opt in to make your data visible.

Except as described in this Privacy Policy, we will not sell, rent or make available your Personal Information to third parties without your permission. Unless in using the website or mobile applications you expressly or impliedly agree to make certain information available, all Personal Information that we collect is kept confidential to the best of our ability, subject to the other terms and conditions of this Privacy Policy. In addition, our employees and contractors who provide services related to our website or mobile applications are obliged to respect the confidentiality of any Personal Information held by us. Our employed staff and contractors are authorised to use your Personal Information only as necessary to provide these services to us.

In the event that we undergo re-organisation or are sold to a third party, any Personal Information we hold about you may be transferred to that re-organised entity or third party in accordance with applicable law. You acknowledge that such acquisitions may occur, and that any acquirer of Wellspace or its assets may continue to use your Personal Information as set forth in this Privacy Policy.

Wellspace may disclose your Personal Information (a) if legally entitled or required to do so (for example if required by law or by a court order or other judicial or administrative proceeding, (b) as otherwise required under any applicable law, rule or regulation and (c) if we believe, in good faith, that such disclosure is necessary to protect or defend our rights or those of others or to assist in the investigation or prevention of illegal activity.

The website may use message boards and messaging forums that will be available to its members. Any information that is disclosed in these areas may become public information and you should exercise caution when using these and disclosing your Personal Information.

Access upon request we will provide you with information about whether we hold any of your Personal Information. If your Personal Information changes or is incorrect or outdated, you may correct, update or amend it by making the change through the “my account” section of the

website. If you no longer desire our service, please contact info@yourwellspace.com to discuss cancelation.

Access and Correction

Upon request,and as required by law, Wellspace will provide individuals with access to Personal Information about them, subject to permitted exemptions. Wellspace will also take reasonable steps to allow individuals to review Personal Information about them for the purposes of correcting such information.

Security

Wellspace will take adequate precautions to protect Personal Information in its possession from loss,misuse,unauthorized access, disclosure, alteration and destruction.

Enforcement

Wellspace has established internal mechanisms to verify ongoing adherence to this Policy, Wellspace commits to resolve complaints about a person's privacy and/or collection or use of personal information. European Union citizens with inquiries or complaints regarding this privacy policy should first contact Wellspace at

Chief Technical Officer

Wellspace

11 Dormer Place, Leamington Spa, UK

paul@yourwellspace.com

Changes to This Policy

This Policy may be amended from time to time, in accordance with the requirements of European data protection laws.

Responsibility

Wellspace expects and requires all applicable colleagues to comply with this Policy and all applicable procedures. Failure to comply may result in a number of serious consequences,

including probation, suspension without pay, reduction in salary,termination of employment, and restitution.

If you are aware of or suspect questionable conduct or potential violations by another colleague, agent, intermediary, customer, or consultant, you should immediately report these concerns to the Legal Department. A Wellspace colleague may raise a concern anonymously through the internet or telephone. Wellspace reserves the right to modify or discontinue this Policy at its discretion at any time without prior notice.

SECURITY POLICY STATEMENT

Wellspace is committed to protecting the company's employees, properties, information, reputation and customer's assets from potential threats in the supply chain. This policy is guided by the company's basic core values, code of conduct, business ethics and supply chain security standards, and it fashions the way we operate throughout the supply chain. All security activities must adhere to the general principles laid down below:

All employees and contractors must always be aware of and take responsibility for the security aspects of the company's business activities;

- Google Endpoint Verification to be used on all employee workstations ,laptops, mobiles and tablets.
- All employee workstations ,laptops, mobiles and tablets must be set to automatically lock after a period of no more than 10 minutes inactivity, the locks should be password protected and make use of biometric locks where available.
- Threats analysis and risk evaluations should be conducted on a regular basis;
- Security procedures and guidelines should be seamlessly integrated with business activities;
- "Incident prevention" must be the first priority;
- Preparedness response plans must be developed and tested to deal with assessed risks rapidly and effectively;
- Security measures and procedures must be subject to regular inspections, validations and verifications by a security auditor so as to maintain high security standards forWellspace.
- The level of professionalism, knowledge and integrity of staff involved in security matters must be tightly controlled;

- Appropriate training plans, customer screening, recruitment, contracting and termination procedures must be established and implemented;
- All incidents, including security breaches and irregularities must be reported and recorded. Corrective action should be taken and followed up through regular verifications to improve the overall security standard.

This policy has been approved by the directors of Wellspace. It will be reviewed, and if necessary revised, annually to keep up to date and will be released on our company website. We welcome interested parties' comments on the enforcement of the policy and the policy itself.

SECURITY TESTING & AUDITS

Cyber Essentials

Wellspace is committed to delivering a safe and secure customer experience and will submit itself for Cyber Essentials Plus certification by the end of 2021.

https://www.ncsc.gov.uk/cyberessentials/overview

ANTIVIRUS/MALWARE PROTECTION

Servers

All servers use Ubuntu 18.04, no applications are run as root therefore no AV is currently required.

Laptop/Workstation

BitDefender is deployed across all user workstations/laptops

SERVER PATCHING

Servers have automated patch management via ManageEnginer Patch Manager Plus. This controls patch management by automating the patch management process,

- Schedule a Patch Scan which scans systems for missing patches

- Based on the severity of the missing patches, we prioritize missing patches with important or critical severity levels. We can patch our machines through manual deployment by creating a patch configuration, or we can automate the deployment.
- Test and Approve - For patches with low or moderate severity, we test those patches in a non-production environment. If they don't cause any problems post-deployment, then they can be rolled out to the production environment.
- View Patch & System Reports - System Health Reports are run to see how our systems are performing post-deployment. The predefined patch management reports show the patch status of our systems, among other things, allowing us to quickly ascertain the security of your network.

USER ACCOUNTS

Principle of Least Privilege

Throughout our systems the Principle of Least Privilege is utilised to reduce the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application. Implementing the P.O.L.P helps contain compromises to their area of origin, stopping them from spreading to the system at large. For example system level database accounts are given read-only privileges to ensure data is not deleted or changed maliciously. User level accounts are restricted to only their own data areas further reducing the risk of data leaks.

User Accounts

All user accounts within the Wellspace organisation are unique to that individual user, no accounts are shared including, but not limited to:

- Servers (Production and Staging)
- Firewalls
- Email
- Deployment Services
- Code Repositories
- Document Repositories

All systems are automatically locked at times of less than 10 minutes and company clear screen policies require individuals to lock their system when leaving the system.

Updating & Revalidation

All admin/user passwords must be changed on an annual basis. Access rights must be verified against the users role to ensure they have access to the correct level of data to carry out their duties but also to ensure compliance as per principle of least privilege.

CLEAR SCREEN POLICY

The Clear Desk and Clear Screen Policy shall communicate the Management's intent to protect information stored in physical and electronic media and minimize risk of unauthorized access. Information is an asset which, like other important business assets, has value and consequently needs to be suitably protected. Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected.

Purpose

To improve the security and confidentiality of information, wherever possible a clear desk policy for papers and removable storage media and clear screen policy for information processing facilities shall be adopted. This shall reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended. The purpose of this policy is to set forth the requirements to ensure that all work areas are clear of company information, whether in electronic or paper form, classified as Level 1 – Confidential (Confidential) or Level 2 – Internal Use (Internal Use) when the work area is unattended.

Definitions

Level 1 – Confidential Information

Confidential information is information whose unauthorized use, access, disclosure acquisition, modification, loss, or deletion could result in severe damage to Wellspace's employees, or customers. Financial loss, damage to Wellspace's reputation, and legal action could occur.

Confidential information is intended solely for use within Wellspace's and limited to those with a "business need-to-know". Statutes, regulations, or other legal obligations or mandates protect much of this information. Disclosure of Confidential information to persons outside of the organization is governed by specific standards and controls designed to protect the information.

Level 2- Internal Use Information

Information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to Wellspace's reputation, violate an individual's privacy rights or legal action could occur.

Scope

IT Assets

This policy applies to all Employees, Contractors, and Third Party Employees, who have access to IT assets of Wellsprace and may be bound by contractual agreements.

Documentation

The Policy documentation shall consist of Clear Desk and Clear Screen Policy and related guidelines.

Document Control

The Clear Desk and Clear Screen Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

Records

Records being generated as part of the Clear Desk and Clear Screen Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Distribution and Maintenance

The Clear Desk and Clear Screen Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Clear Desk and Clear Screen Policy document shall be with the CISO and system administrators.

Privacy

The Clear Desk and Clear Screen Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

Responsibility

The CIO / designated personnel is responsible for proper implementation of the Policy.

Policy

Computers / Computer terminals shall not be left logged-on when unattended and shall be password-protected.

The Security Lock shall be set to activate when there is no activity for 10 minutes.

The Security Lock shall be password protected for reactivation.

Users shall shut down their machines when they leave for the day.

There shall be no screen savers set on for the individual’s desktops and laptops.

Where practically possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

Sensitive or classified information, when printed, shall be cleared from printers immediately.

Individual’s belongings like bags, books, edibles etc. shall be kept in drawers.

Before leaving for the day an individual shall make sure not to leave any paper or belongings on the desk.

Desktops shall have only shortcuts instead of having complete files or folders.

Computer screens shall be angled away from the view of unauthorized persons.

Physical access to the information system device that displays information shall be controlled to prevent unauthorized individuals from observing the display output.

Server rooms and office areas shall remain locked when they are not in use.

All Confidential and Internal Use information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.

All Confidential and Internal Use information must be stored in lockable drawers or cabinets.

File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.

Keys used to access Confidential or Internal Use information must not be left at an unattended work area.

Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.

Passwords must not be posted on or under a computer or in any other accessible location.

Copies of documents containing Confidential or Internal Use information must be immediately removed from printers.

Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy

DATA BREACH RESPONSE POLICY

Scope

This policy covers all systems, servers, workstations, laptops and any additional systems and outputs containing or transmitting Wellspace protected data.

Purpose

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

Policy

Reporting of suspected thefts, data breaches or exposures

Any individual who suspects that a theft, breach or exposure of Wellspace data has occurred must immediately provide a description of what occurred via email to paul@yourwellspace.com or by calling +44808 178 0748. This email address and phone number are monitored by Wellspaces Information Security team. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security team will follow the appropriate procedure depending on the class of data involved.

Confirmed theft, data breach or exposure of Wellspace data.

As soon as a theft, data breach or exposure containing Wellspace data is identified, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of Wellspace, that site will be contacted to have the information removed as soon as possible.

The CTO will chair a response team to handle the breach or exposure. The team will include members from:

ITS Team

C.O.O (Jake Adams)

Additional individuals as deemed necessary by the CTO

If a theft of physical property occurred that contains Wellspace data, ITS should be notified immediately. This team will provide information to the customer regarding how the breach or exposure occurred, the types of data involved, the Wellspace classifications of those data types, any protective measures around the involved data (such as encryption), and the number of internal/external individuals and/or organizations impacted. ITS will handle all communications about the breach or exposure. ITS will work with the appropriate parties to remediate the root cause of the breach or exposure.

Confirmed theft, breach or exposure of Wellspace Public data

The CTO will be notified of the theft, breach or exposure, and will inform the COO as soon as possible. ITS will analyze the breach or exposure to determine the root cause. ITS will work with the appropriate parties to remediate the root cause of the breach or exposure. ITS will also examine any involved systems to ensure that they did not also house any Wellspace Protected data or Wellspace Sensitive data. If the systems are found to also contain Wellspace Protected data or Wellspace Sensitive data, the CTO will be notified and the "Confirmed data breach or exposure of Wellspace Protected data or Wellspace Sensitive data" section of this policy will be invoked.

Questions about this Policy

If you have questions about this policy, please contact the CTO at paul@yourwellspace.com

Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

BUSINESS CONTINUITY/DISASTER RECOVERY POLICY

Fully Managed Databases with standby nodes.

Databases run in our private network, which isolates communication at the account or team level. Requests via the public internet can still reach our database, but only from whitelist specific inbound sources. Data is also encrypted in transit via SSL and at rest via LUKS(Linux Unified Key Setup). Standby nodes are kept up to date in as close to real time as possible, ensuring that any outages that occur are handled seamlessly.

Load Balancers

All our web/access servers are in high availability sets, ensuring that if any go offline for any reason backup servers are instantly available to give seamless access to our services

BackUps

Web/Access servers are backed up weekly, with all production code backed up offline and in private GIT repositories. Databases are backed up daily in addition to real time data

management. All backups are stored in a geographically separate location from the production environment.

DNS Management

All Wellspace's DNS is managed by Cloudflare, providing SSL security and DDoS protection as well as additional intrusion detection.

Floating IP's

We utilise floating IP's in our data centres, this allows us to completely re-create any server from a backup and assign it with that specific services IP address, removing the need for DNS propagation if required.

Monitoring

All servers and endpoints are monitored continuously for:

- Availability
- Memory (RAM and disk)
- CPU

with alerts in place should any of the monitoring criteria be met or exceeded

Disaster Recovery

In the unlikely event of a complete and catastrophic loss of service through natural disaster or other such event, Wellspace aims to be fully functional again within 4 hours at another geographic location. Backups are stored in geographically separate locations and can be moved across data centres in order to restore service.

DATA SANITISATION & ANONYMISATION

Process

For development and testing all data is anonymised before it leaves any production environments, Datasets are replicated on the development environment, this replicated data is then pseudonymized using random name, email, phone number and date of birth generators. This pseudonymized data is then exported and used for development and testing purposes.

Upon completion of testing/dev all data is permanently and irreversibly removed as the virtual database server is destroyed.

All test and development environments are subject to the same security requirements as production servers, with access restricted by IP, SSH Keys etc...

CHANGE MANAGEMENT POLICY

Introduction

The purpose of this policy is to document the way that we manage changes that occur to IT Services including application development in a way that minimises risk and impact to the business. It will also define a Change as understood by IT Services and to describe the accepted Interim Change Management procedure.

Definition of a change

For the purposes of this document and for IT Services, a change will be defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures of any system or service that has the potential to affect the stability and reliability of the infrastructure or disrupt the business.

Changes may be required for many reasons, including, but not limited to:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data centre, etc)
- Unforeseen events
- Periodic Maintenance

Policy

It is the responsibility of IT Services to manage the life cycle of all the systems supporting the business and technical objectives. As such, all the processes and procedures relating to change control and management are set out in this document.

There are two categories of changes that are permitted. They can either be Pre-approved or CAB (Change Advisory Board)-approved and of these categories, there are four types: Minor/Routine, Major/Significant, Emergency/Unscheduled and New Development

NO CAB-approved change should be implemented without:

- A request for change (RFC) being raised via the Change Management Form.(Online at https://yourwellspace.monday.com)
- Approval by the Change Advisory Board (CAB)
- An approved, documented plan of the sequence or steps for implementing and releasing the change into the live environment. This should be stored in an appropriate place e.g. wiki, shared drive, etc
- Evidence demonstrating the fact that this change has been tested in a pre-live/staging environment first.
- A rollback/mitigation plan in case of failure.
- A post-change test being documented to check that the change has been successfully applied.

Incidents

Some incidents may or may not be related to a change, but where a change has caused an incident then it will be possible to trace this back to the person responsible for making that change. The Change Manager will facilitate a review meeting and a report will be generated and fed back to the Change Advisory Board.

Scope

The scope of the Interim Change Management Policy and the procedures contained within it are applicable to all members of IT Services and its authorised colleagues and are related to the management of changes to all IT Services managed live IT systems or services.

Risk

By proactively planning and managing changes for the benefit of users, we should be able to deliver a better and more reliable experience to our customers; this should be done in line with the needs of the business. If not properly controlled, changes could be made which will have a negative impact on the business and could prevent people from fulfilling their roles. Changes could also be made by individuals who are not fully aware of the impact on other areas of the business. All changes should undergo a risk assessment to determine the probability of it occurring and the impact it would have on the business.

Roles and Responsibilities

The Change Manager ensures that changes follow the Change Management Procedure and will review the policy to ensure that it is up to date and relevant. Everyone in IT Services has a potential role and corresponding responsibility with regards to Change Management.

End-Users/Functional Teams:

1. Submitting enhancement requests through the appropriate systems
2. Participating in testing, pre-deployment testing and post deployment testing
3. Timely sign off for the change
4. Verifying that change requests are valid

IT Services Staff as End-Users, Functional Users or Functional User Management:

Responsibility for following the policy.

IT Services Staff Technical Role:

Responsibility to follow prescribed change management processes and procedures.

IT Services Executive:

Overall responsibility for the change management policy and processes contained within it and to ensure that all staff follow it.

Type of Changes

This section defines the different types of changes. Rather than use the confusing ITIL classification of change, IT Services will adopt more meaningful titles to the various types of changes:

- Minor/Routine Change: These are changes that may be done at any time as these have been categorised as low risk to the business and the procedures are known and well documented.
- Examples of this type of are:
    - Application-based security or business needs patches
    - Regularly scheduled maintenance
    - Operating system patches (critical, hot-fixes, and service packs) *
- Major/Significant Change: These are classified as needing approval changes and these must be planned in advance and submitted for approval from the Change Advisory Board (CAB). The change request should also suggest a time for this change to take place via the change form before being carried out. The CAB will have ultimate say if the change goes ahead at the suggested time or not. Detailed in the change request should be the documentation about what work is going to

happen and the perceived benefit and impact to the users. These types of changes should always have a back out plan or mitigating action plan attached.

- Examples of this type of are:
    - Change that results in an interruption to a service, or has a significant risk of an interruption to service
    - Change that results in a business or operational practice change
    - Changes in any system that affect disaster recovery or business continuity
    - Introduction or discontinuance of a service
    - Operating system patches (critical, hot-fixes, and service packs) *
- Emergency/Unscheduled Change: Unscheduled outages (server crashes, etc.) may require immediate attention whenever they happen. The Change logging form should still be filled in, but this could be done retrospectively. Please see the sections on Emergency Change Advisory Board and Emergency/Unscheduled Changes for more information.
- Examples of this type of are:
    - Department or Building is without service
    - A severe degradation of service requiring immediate action
    - A system/application/component failure causing a negative impact on business operations
    - A response to a natural disaster
    - A response to an emergency business need
- New Development: This type of change is specifically for the deployment of new features/functionality, services or applications and is not a fix to a problem.

* This appears in both categories as the impact can vary depending on the content of the patch. The CAB will be able to provide guidance on which category a particular patch fits into and whether it needs approval before applying.

Submitting a Change

1. Go to the change form - https://yourwellspace.monday.com
2. Select the service you are making the change on. If your change affects multiple services then expand as many categories as necessary and select multiple services. Either find it in the service area category or start typing its name in the search box and select it.
3. Fill in the type of change, there are four choices available:
    - Routine – Select this if your change is well known and documented.

    - Fixing a minor fault - Select this if your change is a minor fix i.e. Spelling error
    - New Development – Select this if your changes adds new functionality or features
    - Fixing an urgent / severe problem – Select this if your change is to fix an immediate problem i.e. stopped server.
4. Fill in a brief description of the change, avoid technical jargon and try to keep it plain and easy to understand.
5. Estimate how long the change will take to be made.
6. Fill in the risk to the service category. There are two options:
    - Minimal - Changes that may be done at any time as they have a little or no risk of going wrong and the procedures are well known and documented
    - Significant - Changes that must be planned in advance and need approval. There could be a significant risk to the service.
7. Identify the date and time that the change will be made.
8. Submit the change
9. Change requests will be automatically logged within a Change Database. The CAB meets and reviews applications for change on a monthly basis. It maybe required for you to attend a CAB meeting in order to provide more information or answer questions about the change request.

Change Procedure

All change requests need to be documented and logged, this will be facilitated through the use of the online form. This documentation will be retained centrally within a change request database. For this reason verbal requests and authorisations are not acceptable.

If your change is urgent, then please see the section on Emergency/Unscheduled Changes.

Change Advisory Board (CAB)

The purpose of the change advisory board is to review all CAB-approved change requests and determine whether or not they should be made. In addition, it may determine that certain changes are altered before implementing in order for it to be accepted. The change advisory board membership is based upon the seven different sections of the service catalogue plus at

least one member of IT. For the CAB to be quorate, then at least 2 members should be in attendance but must include either the CTO or Senior Development Manager.

1. Chief Operating Officer
2. Chief Executive Officer
3. Chief Technology Officer
4. Senior Development Manager

Emergency Change Advisory Board (ECAB)

We appreciate that due to the nature of these types of changes that it is not very practical to either wait for group of advisory board members to gather or to seek approval for a change to be made. This is made especially difficult for out of hour's incidents that require immediate or quick changes to be made in order to restore a service. In these circumstances, an appropriate (preferably independent) service manager and member of the executive has the authority to approve a change. It is acknowledged that in some exceptional circumstances that this may not be possible and the authority will then fall on the person making the change. However, the change request form should still be filled in, even if it is retrospectively.

Emergency/Unscheduled Change

In some cases, events are critical enough that they must be rushed though, thereby creating an Emergency/Unscheduled Change. Each situation is different and as much consideration as possible should be given to the possible consequences of attempting this type of change. It is still necessary to obtain sufficient approval for the change, but this may be in the form of discussing the matter with a relevant service manager or section head and logging who it was discussed with and how it was approved.

Pre-Holiday Rule / Leaving Rule

For at least two days prior to annual leave or leaving the business, an IT Services member of staff should only be permitted to make Minor/Routine Changes. If there is an urgent requirement to make an Emergency/Unscheduled change during this time, please ensure that there is sufficient documentation provided and colleagues know where to find it and what the change involves.

Change Freeze Periods

At certain critical times of the year, it will be necessary to impose a non-essential change freeze period. During this time you should only make changes that are deemed essential to either the running of or fixing of a problem with a particular service. If you have the need to make a change during this time, then please follow the instructions sent out with the change freeze dates. If in doubt, contact the change manager. The dates of any change freeze will be communicated well in advance so that you are enabled to plan your work around them.

Cancelling a change

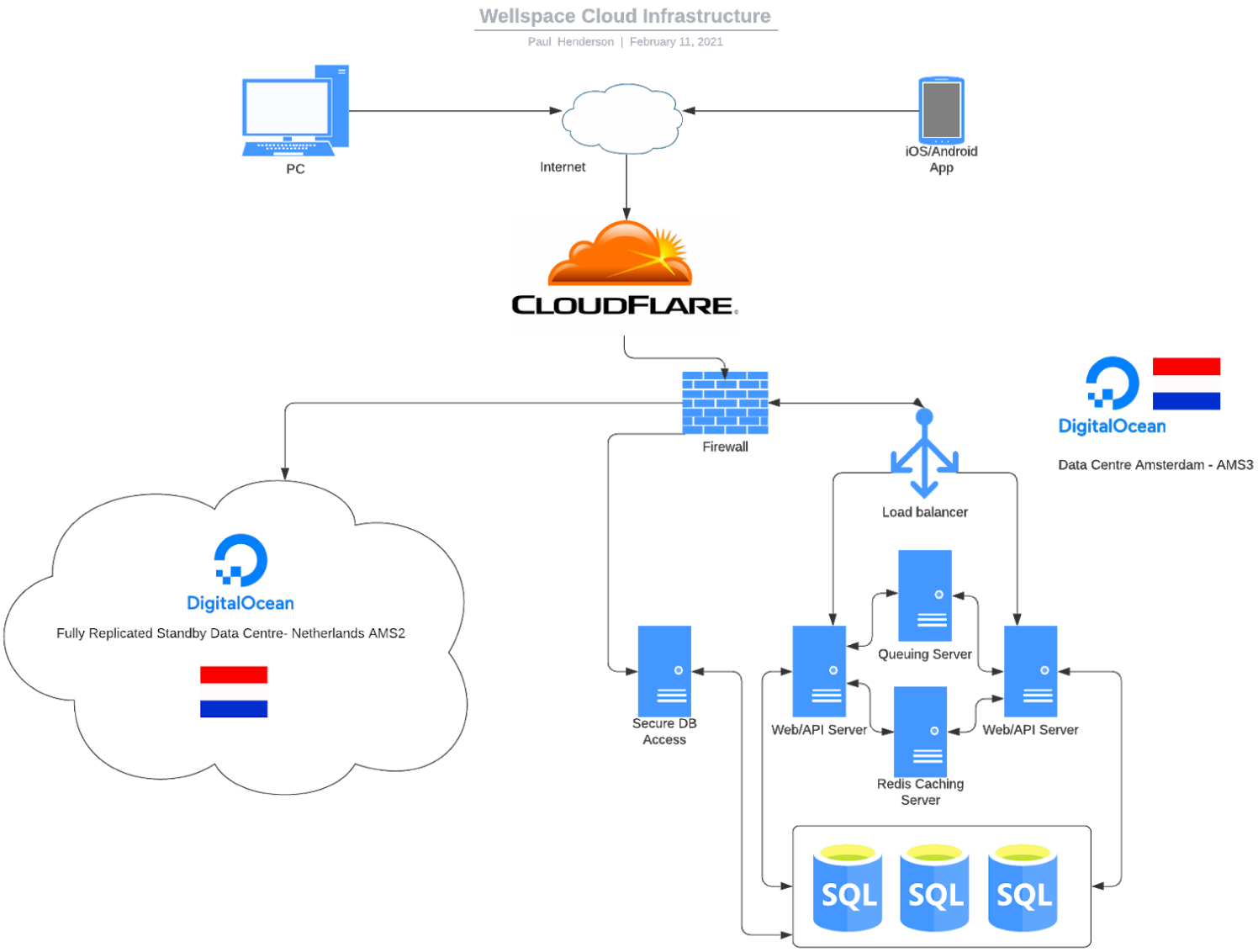
If for any reason you have to cancel or postpone a CAB-approved change, then please do this via the mailing list for change approvers explaining why.

The mailing list is paul@yourwellspace.com , If you need to perform the change again, then please make a new request.

Post Change Checks

After any change has been implemented, the person who is responsible for implementing the change should perform a check to see if it has been successfully applied.

WELLSPACE SYSTEM ARCHITECTURE



DATA BREACH POLICY

Introduction

This Policy and Plan aims to help Wellspace Ltd manage personal data breaches effectively. Wellspace Ltd holds Personal Data about our users, employees, clients, suppliers and other individuals for a variety of business purposes.

Wellspace Ltd is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

A data breach generally refers to the unauthorized access and retrieval of information that may include corporate and / or personal data. Data breaches are generally recognized as one of the more costly security failures of organizations. They could lead to financial losses, and cause consumers to lose trust in Wellspace Ltd or our clients.

The regulations across the various jurisdictions in which Wellspace Ltd operates require Wellspace Ltd to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorized access, collection, use, disclosure, or similar risks.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

As our Chief Technical Officer, Paul Henderson has overall responsibility for the day-to-day implementation of this policy.

Training

All staff will receive training on this policy. New staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar and online training on an annual basis, and covers the applicable laws relating to data protection, and Wellspace Ltd' data protection and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the CTO.

Applicable Legislation Considerations

EU GENERAL DATA PROTECTION REGULATION (EU) 2016/679 (GDPR)

According to the European Commission, Personal Data is: "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Personal Data

Wellspace Ltd defines Personal Data as the broader of the definitions contained in the GDPR.

Wellspace Ltd defines Sensitive Personal Data as the broader of the definitions contained in the GDPR.

Any use of sensitive Personal Data is to be strictly controlled in accordance with this policy.

While some data will always relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute Personal Data unless it is associated with, or made to relate to, a particular individual.

Generic information that does not relate to a particular individual may also form part of an individual's Personal Data when combined with Personal Data or other information to enable an individual to be identified.

Aggregated data is not Personal Data.

Wellspace Ltd gathers Personal Data for two purposes, to identify and protect the data given to us by our customers, and for internal operations.

- Personal Data for health coaching relates to identifiable individual users and may include:
- User profile information such as Full Name, Date of Birth, Mobile telephone number, Address and Personal email address.
- Health-related behavioral data such as step counts, fitness activities, weight, and sleep patterns.

Causes

Data breaches may be caused by employees, parties external to the organization, or computer system errors.

Human Error

Human Error causes include:

- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
- Disclosing data to a wrong recipient
- Handling data in an unauthorized way (eg: downloading a local copy of personal data)
- Unauthorized access or disclosure of personal data by employees (eg: sharing a login)
- Improper disposal of personal data (eg: hard disk, storage media, or paper documents containing personal data sold or discarded before data is properly deleted)

Malicious Activities

Malicious causes include:

- Hacking incidents / Illegal access to databases containing personal data
- Hacking to access unauthorized data via the Coaching App or API
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
- Scams that trick Wellspace Ltd staff into releasing personal data of individuals

Computer System Error

- Computer System Error causes include:
- Errors or bugs in Wellspace Ltd' Application, or API
- Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems
- Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

Under the GDPR, the CTO is legally obliged to notify the Supervisory Authority within 72 hours of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (Article 34). In addition, Wellspace Ltd must notify any affected clients without undue delay after becoming aware of a personal data breach (Article 33).

However, Wellspace Ltd does not have to notify the data subjects if anonymized data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudo-anonymisation techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach (Article 34).

Data Breach Team

The Data Breach Team consists of the CTO / COO with Paul Henderson acting as our CTO. Paul has the responsibility to make all time-critical decisions on steps taken to contain and manage the incident.

The Data Breach Team should immediately be alerted of any confirmed or suspected data breach via email:

Paul Henderson (paul@yourwellspace.com) and Jake Adams (jake@yourwellspace.com)

The notification should include the following information, where available:

Extent of the data breach

- Type and volume of personal data involved
- Cause or suspected cause of the breach
- Whether the breach has been rectified
- Measures and processes that the organization had put in place at the time of the breach
- Information on whether affected individuals of the data breach were notified and if not, when the organization intends to do so
- Contact details of Wellspace Ltd staff with whom the supervisory authority can liaise for further information or clarification

Where specific information of the data breach is not yet available, Wellspace Ltd should send an interim notification comprising a brief description of the incident.

Notifications made by organizations or the lack of notification, as well as whether organizations have adequate recovery procedures in place, will affect supervising authorities' decision(s) on

whether an organization has reasonably protected the personal data under its control or possession.

Responding to a Data Breach

Data Breach Management Plan

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team should immediately activate the data breach & response plan.

Wellspace Ltd' data breach management and response plan is:

- Confirm the Breach
- Contain the Breach
- Assess Risks and Impact
- Report the Incident
- Evaluate the Response & Recovery to Prevent Future Breaches

Confirm the Breach

The Data Breach Team (DBT) should act as soon as it is aware of a data breach. Where possible, it should first confirm that the data breach has occurred. It may make sense for the DBT to proceed Contain the Breach on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

Contain the Breach

The DBT should consider the following measures to Contain the Breach, where applicable:

- Shut down the compromised system that led to the data breach.
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (eg: remotely disabling / wiping a lost notebook containing personal data of individuals.)
- Prevent further unauthorized access to the system.
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

Assess Risks and Impact

Knowing the risks and impact of data breaches will help Wellspace Ltd determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

- Risk and Impact on Individuals

  How many people were affected? A higher number may not mean a higher risk, but assessing this helps overall risk assessment.

- Whose personal data had been breached?

  Does the personal data belong to employees, customers, or minors? Different people will face varying levels of risk as a result of a loss of personal data.

- What types of personal data were involved?

  This will help to ascertain if there are risks to reputation, identity theft, safety and/or financial loss of affected individuals.

- Any additional measures in place to minimize the impact of a data breach? eg: a lost device protected by a strong password or encryption could reduce the impact of a data breach.

Risk and Impact on organizations

What caused the data breach?

Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.

When and how often did the breach occur?

Examining this will help Wellspace Ltd better understand the nature of the breach (e.g. malicious or accidental).

Who might gain access to the compromised personal data?

This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if personal data is acquired by an unauthorized person.

Will compromised data affect transactions with any other third parties?

Determining this will help identify if other organizations need to be notified.

Incident Reporting

Wellspace Ltd is legally required to notify affected individuals if their personal data has been breached. This will encourage individuals to take preventive measures to reduce the impact of the data breach, and also help Wellspace Ltd rebuild consumer trust.

Who to Notify

- Notify individuals whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify GDPR especially if a data breach involves sensitive personal data.
- The relevant authorities (eg: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (eg: hacking, theft or unauthorized system access by an employee.)

When to Notify

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved

How to Notify

- Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify

- How and when the data breach occurred, and the types of personal data involved in the data breach.
- What Wellspace Ltd has done or will be doing in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
- Contact details and how affected individuals can reach the organization for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

Evaluate the Response & Recovery to Prevent Future Breaches

After steps have been taken to resolve the data breach, Wellspace Ltd should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the data breach.

Operational and Policy Related Issues

- Were audits regularly conducted on both physical and IT-related security measures?
- Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
- Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
- Were the methods for accessing and transmitting personal data sufficiently secure, eg: access limited to authorized personnel only?
- Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data?
- Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data?
- Is there a need to develop new data-breach scenarios?

Resource Related Issues

- Were sufficient resources allocated to manage the data breach?
- Should external resources be engaged to better manage such incidents?
- Were key personnel given sufficient resources to manage the incident?

Employee Related Issues

- Were employees aware of security related issues?
- Was training provided on personal data protection matters and incident management skills?
- Were employees informed of the data breach and the learning points from the incident?

Management Related Issues

- How was management involved in the management of the data breach?
- Was there a clear line of responsibility and communication during the management of the data breach?

Monitoring

Everyone must observe this policy.

The CTO has overall responsibility for this policy.

The CTO will review and monitor this policy regularly to make sure it is effective, relevant, and adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.