Policy: Security

Department: IT

Date: **Approved October 2016** **Review Date:** **January 2018**

1.0 Purpose

This policy defines how seriously we take the security of your data at 110% Ltd. As transparency is one of the principles on which our company is built, we aim to be as clear and open as we can about the way we handle security.

If you have additional questions regarding security, we are happy to answer them. Please write to **info@110percent.io** and we will respond as quickly as we can

2.0 Scope

This policy applies to:

- All personal data held and processed by 110% Ltd.
- All employees of 110% Ltd who are granted access to personal data.
- All contractors, suppliers, 110% Ltd partners and external collaborators and visitors who may be authorised to access 110% Ltd held personal data.
- All locations from which personal data is accessed including home and off-site/ remote use.
- Any other parties who may be holding personal data on behalf of 110% Ltd.
- This policy works in conjunction with 110% Ltd.'s policies when 110% Ltd is used as a messaging medium.

3.0 Confidentiality

We place strict controls over our employees' access to the data you and your users make available via the 110% services, as more specifically defined in your agreement with 110% covering the use of the 110% services ("**Customer Data**"), and are committed to ensuring that Customer Data is not seen by anyone who should not have access to it. The operation of the 110% services requires that some employees have access to the systems which store and process Customer Data. For example, in order to help diagnose a problem you are having with the 110% Ltd services, we may need to access your Customer Data. These employees are prohibited from using these permissions to view Customer Data unless it is necessary to do so. We have technical controls and audit policies in place to ensure that any access to Customer Data is logged.

All of our employees and contract personnel are bound to our policies regarding Customer Data and we treat these issues as matters of the highest importance within our company.

4.0 Personnel Practices

110% Ltd conducts background checks on all employees before employment, and employees receive security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our comprehensive information security policy covering the security, availability, and confidentiality of the 110% services.

5.0 Compliance

The following security-related audits and certifications are not yet applicable to the 110% services as we do not hold or process client's financial data:

- **Service Organization Control (SOC) Reports:** 110% Ltd has at this time no need to hold or process credit card information
- **PCI**: 110% Ltd is not currently a PCI-certified Service Provider and has not completed the Payment Card Industry Data Security Standard's SAQ-A. We currently neither hold nor process credit card information.

The environment that hosts the 110% Ltd services maintains multiple certifications for its data centres, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, please visit the AWS Security website and the AWS Compliance website.

6.0 Data Encryption in Transit and At Rest

The 110% Ltd services support the latest recommended secure cipher suites and protocols to encrypt all traffic in transit. Customer Data is encrypted at rest.

We monitor the changing cryptographic landscape closely and work promptly to upgrade the service to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

7.0 Availability

We understand that you rely on the 110% services to work. We're committed to making 110% Ltd a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers or even entire data centres. Our operations team tests disaster-recovery measures regularly and staffs an around-the-clock on-call team to quickly resolve unexpected incidents**.**

Our systems use the AWS Cloud infrastructure is built around Regions and Availability Zones ("AZs"). A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centres, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones provide the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data centre. The AWS Cloud operates 44 Availability Zones within 16 geographic Regions around the world.

Our services built on this infrastructure have an SLA in excess of 899.9% uptime

8.0 Disaster Recovery

Customer Data is stored redundantly at multiple locations in our hosting provider's data centres to ensure availability. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. Customer Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected.

9.0 Network Protection

Customer Data is stored redundantly at multiple locations in our hosting provider's data centres to ensure availability. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. Customer Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected.

10.0 Host Management

We perform automated vulnerability scans on our production hosts and remediate any findings that present a risk to our environment. We enforce screens lockouts and the usage of full disk encryption for company laptops.

11.0 Logging

110% maintains an extensive, centralized logging environment in its production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about the 110% services. These logs are analysed for security events via automated monitoring software, overseen by the security team

12.0 Incident Management and Response

In the event of a security breach, 110% will promptly notify you of any unauthorized access to your Customer Data. 110% has incident management policies and procedures in place to handle such an event

13.0 External Security Audits

We contract with respected external security firms who perform regular audits of the 110% services to verify that our security practices are sound and to monitor the 110% services for new vulnerabilities discovered by the security research community. In addition to periodic and targeted audits of the 110% services and features, we also employ the use of continuous hybrid automated scanning of our web platform.

14.0 Product Security Practices

New features, functionality, and design changes go through a security review process facilitated by the security team. In addition, our code is audited with automated static analysis software, tested, and manually peer-reviewed prior to being deployed to production. The security team works closely with development teams to resolve any additional security concerns that may arise during development.

15.0 Monitoring and auditing

This policy and its implementation will be subject to internal monitoring and auditing throughout the 110% Ltd, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. 110% Ltd will also undertake appropriate benchmarking and external auditing exercises.

9.0 Associated documents

Please refer to:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Freedom of Information Policy
- Staff Privacy Notice
- Client Privacy Notice
- Personal Data Request procedures
- Data Retention and Archiving Policy

10.0 Review of policy

This policy will be reviewed at least every two years or when there are significant changes to it.

11.0 Contact list for queries related to this policy

Data Protection Officer
Chief Information Officer

12.0 Authority for this policy

Senior Management Team