branch

Information Security & Privacy Standards

Branch Metrics, Inc. is committed to adopt and adhere to the following technical and organizational security measures for software development, business operations and data privacy to provide a secure and safe platform service to our customers:

Governance

- Branch shall implement and maintain an Information Security Management System (ISMS) that meets or exceeds industry standards and that includes, without limitation, appropriate policies, governance structures, staffing, monitoring and assessment procedures.
- Security policies shall be approved by the Chief Operating Officer (COO) or the Information Security Management Committee (ISMC). Any exception must be authorized by the Head of Security or ISMC.
- Branch shall update security policies at least annually.

Workplace Security

- Branch shall install a visitor check-in system. All visitors must sign in at the front desk, and the visitor management application will notify the hosting employee to pick up the visitors. The visitor management application will issue a visitor badge. While visiting office premises, visitors must be accompanied by the hosting employee and wear their visitor badge in a publicly visible fashion at all times.

- Branch shall implement and maintain a secure mobile device management system to secure assets and information access for work. Company-issued devices and laptops are secured using a tested image and are protected using anti-virus and malware scanning software. To protect business data from data theft or exploit, external USB storage devices for laptops are prohibited (mitigated by mobile device management tool). Under Branch's BYOD (Bring Your Own Device) policy, personal mobile devices are required to access a separate guest wifi network if used in the office.

Physical Security

- Branch shall implement and maintain a program to ensure personnel physical access is revoked immediately upon termination or when access is no longer required.
- Employees must use an issued security access card to access office premises. Branch shall use physical locks inside the office building to secure network equipment and company assets. Access to server rooms should be restricted to authorized IT administrative staff. Security surveillance recordings are for review in case of any incident.

Organizational Controls

- Branch shall implement and maintain policies and procedures, which shall be documented and approved by its senior management, to support the hiring, termination, code of conduct, ethics and background screening of all employees and contractors.
- Branch shall perform a background check using a reliable third-party service for each employee.
- Branch shall implement and maintain a security awareness program for employees, which provides basic IT security standards (during employee on-boarding), annual privacy and security awareness training, and individual personnel acknowledgment of intent to comply with corporate security policies.

Network Security Measures

Authentication and Password Policy Control

- Branch shall implement and maintain strong password management policies for all end user and system accounts related to the processing environment. Such procedures must follow recognized industry best practices in their configuration and management, including length and structure (commonly referred to as strong passwords).
- Branch shall implement a strong and complex password policy enforced for employees and developers. This should require at least 8 characters in length, including at least 1 uppercase character, 1 lowercase character, 1 number, and 1 special character. For employees, an industry-strength Mobile Device Management tool is used to enforce password policy in company-issued laptops. MFA (Multi-factor Authentication) is required to access Branch Metrics dashboard and applications.
- Branch shall implement an account lockout policy when users exceed the threshold of invalid login attempts.

System and Data Access

- Branch shall implement and maintain a secure system access mechanism and a remote access mechanism. Only authorized production support members and customer data administrators can access Branch's production systems backend and customer data on an as-needed basis via secured channels using virtual private network (VPN), jump boxes, secure shell (SSH) and multi-factor authentication (MFA).
- Branch's Web services require the use of service accounts and secure API tokens.

Logical Data Access

- Branch shall implement and maintain a logical system access provisioning process that meets or exceeds industry standards for all systems that access, process or store customer data and

confidential information.

- Branch shall implement role-based security access.
- Branch shall implement and maintain a periodic logical access control review.

Operations Security Measures

Secure Software Development Lifecycle Process

- Branch shall implement a secure software development lifecycle process using agile development methodology, and periodically review security issues identified from static code analysis (SAST), Web application vulnerability scanning (DAST), penetration testing, and container security vulnerability scanning automated in the build pipeline.
- Branch shall engage third party professional security firms to perform network and application penetration testing in production environments annually. In addition, Branch will use security researchers from crowdsourcing communities to identify exploits and security vulnerabilities.

Risk Management

- Branch shall implement and maintain a vendor and technology risk assessment strategy and risk mitigation methodology. The due diligence process will ensure systems security and data privacy details are reviewed, and security risks are mitigated before adoption.

Backup and Restore

- Branch shall implement and maintain data backup and restore processes to secure business data. Daily backups (snapshots) of data are made and stored in redundant locations. Only authorized personnel may access or restore any data from the backup datasets.

Security Monitoring and Logging

- Branch shall implement comprehensive system monitoring for Branch's cloud applications and microservices.
- Branch shall implement vulnerability and network intrusion detection controls. These controls will generate proactive alerts to notify the platform infrastructure team about any system events and suspicious activities that may be potential security incidents. Detailed logging and audit reports are available upon request for security incident diagnosis and forensics.
- Branch shall implement and maintain security information and event management (SIEM) system. All system logs are redirected to a central infrastructure for event tracking, diagnosis and audit trail. In addition, with the use of SIEM, security team members can continuously monitor for any possible suspicious application behavior and unusual system events and respond timely to active and emerging security threats.

Security Incident Response Process

- Branch shall implement and maintain a security incident response program. The security incident response program shall define steps to be coordinated with the cross-functional incident response team in order to mitigate security incidents in a timely manner. All verified security incidents will be reported to the security incident response team in a timely manner. Depending on the levels of response, and pursuant to the applicable customer agreement, customers will be notified timely about the status and the remediation.
- Branch shall test the security incident response process annually.

Business Continuity

- Branch shall implement and maintain a business continuity program that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions ("Business Continuity Program").

- Branch shall conduct a business continuity test every twelve (12) months, including a review of the Business Continuity Program, roles and responsibilities, business documentation requirements, recovery strategies, Mean Time to Recovery (MTTR), Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), testing strategy and frequency.
- Branch shall implement and maintain a disaster recovery program that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions.

Change Management

- Branch shall implement and manage a change management system for planned and emergency software changes. There will be a workflow approval process in place to ensure change requests are prioritized and assigned.
- Branch shall implement a security patch management program. Software and security updates are pushed out periodically and on-demand. Critical security updates will be applied in a timely manner to mitigate any immediate security risks.
- Branch shall implement and manage a configuration management system. Configuration of systems and services is performed automatically by programs vetted for security deficits.

Data Security and Privacy Measures

Data Encryption and Integrity

- Branch shall provide industry standard encryption of customer data and confidential information in transit over public or leased circuits.
- Branch shall provide industry standard encryption of customer data and confidential information at rest on local laptops, mobile devices, shared drives, as well as on backend data stores.

- Branch shall implement and maintain logical data segregation that meets or exceeds industry standards to ensure customer data and confidential information is not viewable by unauthorized users.
- Branch shall implement input and output validation for data protection in the dashboard application. Business data is validated and checked for integrity in the backend microservices and in the API Web services. A data loss prevention tool shall be deployed in Branch's backend storage infrastructure to ensure data integrity.

Data Management and Protection

- Branch has implemented different data protection controls to ensure data privacy of customer data in accordance with applicable law. This includes protecting data at rest (data encryption), data in transit (secure data transport) and role-based system access control. Data access is restricted to authorized personnel, and production backend systems can be only accessible using MFA, VPN and company-issued laptops.
- Branch shall have the necessary processes and procedures in place to execute Data Subject Requests regarding personal data in accordance with applicable law in order to meet applicable legal requirements.
- Branch shall follow industry security best practices (e.g. Amazon, NIST) to destroy storage media, including cloud storage and also laptop hard drive before disposal.

Data Privacy

- Branch maintains a documented data privacy statement that describes what data Branch collects, how it is used and how it is shared available at https://branch.io/privacy.