WHITEPAPER

INFOSECURITY AND SOC 2 AT FIRST FACTORY

FIRST FACTORY

The standardization of our software development practices and the maturing of our security measures are primary points of focus at First Factory. In order to bring more structure and skills related to information security awareness and preparedness into our organization, we engaged with Fractional CISO to serve as our dedicated virtual CISO (vCISO). Part of our goal, beyond making the improvements to our policies and procedures to mitigate info security risks and establish protocols for responding to and recovering from incidents, was to be positioned to acquire a SOC 2 attestation.

ACHIEVING SOC2 TYPE 1 COMPLIANCE

SOC 2 (Service Organization Control 2) is a framework for managing and securing sensitive information relevant to technology organizations such as ours. The ability to demonstrate the existence of policies and compliance with the procedures that support those policies, as they are related to handling sensitive information, is the core of what the SOC 2 auditors are looking for. The SOC 2 Type 1 report provides an overview of First Factory's systems and the suitability of the design of our controls at the time of assessment. The attestation we received from the auditing firm, Marcum Accounting and Advisors, showcases our ability to meet relevant trust service criteria, with an emphasis on security, availability, and confidentiality. The report, which we will share upon request, includes our description of services and the evaluation confirming the suitability of our controls.

Marcum used the Committee of Sponsoring Organizations (COSO) framework when evaluating our operation. With this framework, they assessed performance against the following categories: Control Environment, Enterprise Risk Management, Control Activities, Information and Communications, and Monitoring. The affirmation received from Marcum indicates that, as a software development service provider, First Factory has demonstrated strong and consistent adherence to legal and ethical requirements as well as risk assessment and management.

THE FOUNDATION FOR SECURITY

The preparation for the evaluation was lengthy and detailed. Our internal Information Security Steering Committee (ISSC) eagerly embraced the process, not because we looked forward to an audit but because each internal evaluation allowed us to identify areas of improvement and further the company's security posture. Through each learning, we shared the findings with our employees, thus improving infosec awareness across the organization. As a nearshore software development company, one can imagine how important it is for each member of our team to safeguard our clients' sensitive and confidential information. Working with approximately forty clients at any given moment and needing to adhere to their policies and security features in addition to our standards and protocols adds complexity when ensuring that our employees and systems operate securely and consistently. Our employees also apply what they learned through our security awareness training to our client's products and services, further improving their security position and strengthening those partner relationships.

We began the audit by demonstrating a commitment to integrity and ethical values. We conduct background checks for all applicants as a condition of employment. Other employment requirements include all staff reading and signing a Confidentiality and Non-Disclosure Agreement, an Acceptable Use Policy, and a few other specific InfoSecurity documents in addition to acknowledging compliance with over two dozen InfoSec policies. We have demonstrated separate and sufficient management oversight and have a clear corporate structure with well-defined roles and responsibilities. We established redundancies for key positions and built them directly into our operating model.

PARTNER INFOSEC COMMITMENTS

New business partners and third-party vendors are also subject to nondisclosure agreements or other contractual confidentiality and privacy provisions and are evaluated on their security profile and ethical values. As with all relationships, First Factory evaluates behaviors and has processes in place to address breaches in confidence. Those found in violation of these conditions, or those who refuse to provide transparency into the safeguarding of confidential information, are offboarded—at which point we ensure that any sensitive or proprietary data is appropriately transferred and deleted.

Our vCISO team conducts formal risk assessments to determine risk levels, acceptance, and mitigation planning. Fractional CISO also conducts internal audits and facilitates tabletop scenarios. First Factory engages with a third-party

vendor who conducts annual vulnerability/penetration testing of our environments during the examination window and offers corrective action for any high/critical findings. These Pen Test results are available on request. Our vCISO conducts an annual security incident response test to demonstrate the effectiveness of our procedures.

ACTIVE SECURITY PREPAREDNESS

Internally, we have quarterly control audits that review the comprehensiveness and effectiveness of our controls to secure the business and product environments, technologies, and data. Business Continuity Planning (BCP) and Disaster Recovery (DR) procedures are in place and are adhered to in real and simulated BCP/DR scenarios. We require secure data transmission protocols and a robust data classification and handling system, including data backups that are systematically scheduled. And, of course, we have cybersecurity insurance to mitigate the financial impact of a breach or other incident.

There is a host of other security criteria evaluated in the SOC 2 audit—too many to detail. Some of the highlights include reviewing our Access Management Cloud Services that manage authentication and prevent unauthorized access to company applications, and the onboarding and offboarding workflows and logs that prove the work is done quickly and consistently. Multi-factor authentication, password mandates, biometric access to facilities, and mobile device management (MDM) are some of the ways access to sensitive materials is appropriately maintained. The MDM solution is also utilized to restrict the use of removable media and to alert administrators of unapproved software installation and viruses. Through the MDM, we force vendor security patch updates. Should a device be stolen or compromised, we remotely wipe the contents of the device, lock the device down, and track the device to assist the authorities. All of the aforementioned measures, along with the proactive and transparent communication of these events to our customers, are some of the tools and processes we rely on to maintain a high standard of security and have helped earn us our SOC 2 attestation.

REMAINING STRONG TOGETHER

We are proud of our internal team for taking these security measures seriously and for their continued commitment to staying abreast of Infosecurity measures and practices. We are grateful to our partners who helped shepherd us to this point. We will continue to strengthen our infosec position and will use this SOC 2 attestation as an early milestone in our infosecurity journey.

In spite of the increase in phishing campaigns, ransomware, and malevolent agents, with First Factory as your software development partner, the future can be secure.

First Factory is a Nearshore Software Development partner with twenty-plus years of experience helping companies maximize their digital products' performance, user adoption, and financial goals. Through relationships with hundreds of clients across numerous industries, the First Factory team of over 220 maintains expertise across all major technologies and supplies a full suite of software development services, including engineering, quality assurance, project management, and UX/UI design.

With a lifetime eNPS of 80, First Factory is an employer of choice in the Costa Rican development community and has made the Inc 5000 list of fastest-growing private companies in the US four years in a row. Deeply ingrained in the company culture is the commitment to quality, honesty, and integrity, which are core to long-term relationships with clients.

If you have a product development need, consider the nearshore development team at First Factory for design, development, project management, and product ideation.

Contact us at +1.646.688.5070 or firstfactory.com/contact-us.