QuickBooks Online
Security White Paper
March 2018

Introduction

At Intuit® QuickBooks® Online (QBO), we consider the security of your information as well as your customers' and employees' data a responsibility that is aligned with a key Intuit value: Integrity without Compromise. You have trusted us to hold your data securely and we take this responsibility seriously.

Security is a shared responsibility. This document describes some of the security controls Intuit has in place to protect your data. Additional information for what you can do to protect your company data is available online at https://security.intuit.com/index.php.

Governance

Intuit has a comprehensive set of security policies and procedures. Topics include:

- Security Oversight
- Data Classification
- Data Handling
- Logical Access Management
- Physical Security
- Development and Quality Assurance
- Operational Security
- Security Incident Response
- Payment Card Processing
- Third Party Management

QBO and supporting systems handling payment card data are annually assessed to the Payment Card Industry Data Security Standard by a qualified, third-party security assessor. This assessment reviews practices such as data retention, networks and systems hardening, incident response, data handling and security, access control and monitoring and security policies and procedures.

As a key part of Intuit's Small Business Group and Self-Employed Group, QBO is subject to a number of other compliance assessments and audits including:

- Sarbanes Oxley (SOX) Application and IT General Controls Audits;
- Internal Audits; and
- NACHA Audits.

Risk Assessment

Intuit conducts annual risk assessments with quarterly check-ins to identify and address critical business risks. In addition, the QBO team does bottoms-up risk assessments on a continual basis. For example, before any changes are released to the product, they are reviewed and tested thoroughly, in addition to undergoing regular vulnerability scans, pen tests, internal and external audits on QBO and the Intuit services and offerings it depends on.

Authentication

Different multi-factor authentication (MFA) strategies using things only known to the account owner help safeguard against inappropriate account access and validate your identity for sensitive operations (password reset, making or receiving payments, etc.). QBO also uses CAPTCHA and other techniques to protect against automated denial of service (DoS) attacks.

Access Control

QBO provides granular role-based security so that only you or your designee can specify who can access your data and what level of privileges can be granted to different users. We follow a strong password and multi-factor authentication policy across all environments.

You control who accesses your financial data, and what they can see and do with it. Each person you invite to use QBO must create a unique login. Multiple permission levels let you limit the access privileges of each user. For example, you may want your part-time contractor to be able enter work hours, but not access your latest P&L charts.

QBO provides an audit trail that tracks the actions taken by different users. This can help you keep track of who does what with your data.

Access to systems, services, and your data follows the principle of least privilege. This means personnel responsible for data backups (as one example) only have access rights sufficient for that purpose.

We segregate roles within our development and production teams. Production access requires appropriate levels of authorization. For example, developers do not have access to production systems and operations personnel do not have access to source code.

Security Awareness Training

All Intuit employees are required to undergo security awareness training on initial hire and annually thereafter. The training covers general security topics, including personnel and physical security, social engineering, IT security controls in place at Intuit (e.g., antivirus, security policies), and privacy best practices. Additional job-related training may be required, depending on the specific duties assigned to individuals. These include secure coding and testing techniques and operations monitoring and response. Our Intuit software development teams also attend frequent technical seminars designed to help them stay on top of secure coding practices.

Data Security

No single measure can effectively provide complete security, so at QBO, we employ a strategy called “defense in depth,” a layered approach with multiple security measures in place to help protect your data. We take specific precautions to provide security while your data is in transit from your computer to our servers, as well as while it is being processed and stored in our data centers.

Let’s start with your data as it leaves your browser. QBO establishes a secure connection to your browser, indicated by the small padlock symbol displayed on your screen (the exact location varies by browser). The padlock symbol denotes a secure connection using TLS (Transport Layer Security) technology to encrypt your data over the Internet. Intuit uses the highest level of protection your browser allows to help protect your data in transit.

Your data stays encrypted as it passes through Intuit-managed firewalls. It is processed and stored on dedicated systems protected via tokenization and encryption per National Institute of Standards and Technology (NIST) guidance.

Information Protection Processes and Procedures

Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.

We follow a strict set of guidelines and practices to help protect your private information. We will not, without explicit permission, sell, publish or share data entrusted to us by a customer that identifies the customer or any person. Our employees are trained on how to keep data safe and secure. Intuit is a licensee of the TRUSTe Privacy Program, an independent, nonprofit organization committed to the use of fair information practices, and is Privacy Shield certified (www.privacyshield.gov/Program-Overview). You can read more about our privacy practices on our Privacy Statement web page (https://security.intuit.com/privacy).

We incorporate security throughout our standard Software Development Lifecycle (SDLC). This includes threat modeling of architecture and designs, security code reviews, static automated analysis, security vulnerability scans, compliance scans and penetration testing by internal and external security experts. These activities leverage technologically advanced automation tools and industry-vetted security frameworks to ensure quality and security of QBO and your data. This includes regular patching for known vulnerabilities published by security vulnerability tracking authorities, such as Mitre and the National Vulnerability Database.

Protective Technology

Intuit takes service availability very seriously. QBO is designed to survive a major disaster: We have redundancy within and across at least two geographically separated data centers.

QBO is hosted on data centers rated the highest Tier-4 category. Each data center has high physical security, redundancy, and backups for power and cooling. This includes infrastructure components to avoid single points of failure. All web, application, and data servers are spread across multiple isolated fault domains built on best-in-class network and server virtualization technology.

Offices and data centers are guarded by onsite security personnel. We enforce access card-based entry to each building and 24/7 perimeter vigil and control. Data center security maintains even stricter access controls.

Data is replicated securely between the data centers over multiple telecommunication carriers using industry-standard replication technology. Data synchronization latency between data centers is maintained at less than 5 minutes. Intuit engineers have implemented extensive automation to facilitate non-disruptive switchovers between data centers as often as every other week.

Security Monitoring

Information systems and assets are monitored for intrusion, unauthorized access, unexpected file changes, unplanned spikes in activity and other events, as well as to verify the effectiveness of protective measures. Our Security Operations Center (SOC) is staffed 24x7, 365 days a year to monitor activities across all Intuit applications and services.

Intuit has a global Incident Management Team. This team includes senior executives, product engineers and members of our Security Operations Incident Response Team, and can engage the right business contacts so any identified incidents are resolved quickly. For day-to-day incident event monitoring and response our Security Operations team is responsible for monitoring, opening tickets and following potential incidents and events to resolution.

Business Continuity and Disaster Recovery

QBO runs in asymmetric “active-active” mode, in which processing is mirrored across our data centers to ensure real-time replication of all systems and data. If something should happen in one data center, another one is ready to take over within moments. We backup our systems at least once a day and use multiple suppliers for critical operational functions such as telecommunications lines. Our data centers are geographically separated, to minimize the chance that a natural disaster in one location might prevent you from accessing your data.

Bottom Line

At Intuit® QuickBooks® Online (QBO), we know your data is important to you. We hope the information in this white paper gives you insight into how we approach data security.