How Secure is Wurk?

Last Modified on 02/09/2022 11:40 am EST

When evaluating any vendor's cloud offering, you need to be confident that your application(s) and data are being maintained at a state-of-the-art data center facility engineered to incorporate multiple levels of security and redundancy, thereby ensuring maximum availability of your HCM solution.

For a more basic overview, see our website.

Wurk Security and Auditing

The Wurk solution, which is built on the Kronos® Workforce Ready® platform, has achieved the American Institute of Certified Public Accountants ("AICPA") SSAE 16 SOC 1 Type II and AT101 SOC 2 Type II criteria for security, availability, and confidentiality. The cloud environment undergoes an annual audit by an independent Tier 1 auditing firm that publishes the SOC Type II reports attesting to the suitability and operating effectiveness of the controls in place. Kronos has certified its compliance with the EU/US Privacy Shield Framework.

Because Wurk is hosted in the cloud, you get 24x7 access to your solution. You gain peace of mind knowing that experienced Wurk Implementation consultants are managing the solution infrastructure, as well as your applications and employee data, to help ensure high availability, reliable performance, and multi-layer security. In addition, because upgrades and add-ons take place in the cloud, you enjoy instant access to the latest software enhancements to help you manage your workforce for the best results.

At Wurk, we understand that SaaS offerings must be backed by a world-class technology infrastructure that customers can count on day in and day out. That's why the Wurk cloud environment provides the highest levels of data security, system uptime, and built-in redundancy. Our primary and secondary data centers — among the most secure, connected, and compliant facilities in the industry — are designed from the ground up to help ensure the availability and security of your Wurk data, and to deliver seamless business continuity across virtually any circumstances. As a result, your organization can rely on secure, continuous access to the automated tools and high-quality information needed for effective workforce management.

User Access

Your system requires all users to log in from a web browser or mobile device via encrypted Transport Layer Security (TLS) sessions using port 443. You can also use TLS to encrypt data transmission when you provide a digital ID certificate from a third-party vendor (If your company uses InTouch clocks, these terminal connections are Ethernet-based using port 80 or 443). The first time your users log in, they use a link from your administrator (sent by email) that requires them to set up a user name and password. First-time login requires "Two Factor Authentication", meaning users must verify their identity by a second method (email

or text message) and enter a verification code that is automatically generated during the process. Wurk uses industry-standard, modern hashing algorithms to secure your user passwords and they are never stored in clear text. Once your users have set up their credentials, they must enter these every time they log in. Like all industry-standard secure systems, Wurk will lock them out if they make too many failed attempts to log in.

Wurk also requires that the employees' Manager or Administrator approve their first attempt to log in within 72 hours, adding a human factor to the security process. If their login is not approved, they will be locked out.

About Our Primary Data Center

Wurk is hosted at a secure off-site data center. This world-class data center facility delivers cloud, managed hosting, and colocation services while providing superior integrated hosting services, carrier/network connectivity, and 24x7 security. This data center specializes in meeting industry-specific compliance standards to help ensure the ongoing security and integrity of Wurk. The primary data center is constructed and equipped to meet the most stringent security mandates for comprehensive physical, network, and policy-based security.

System Uptime

Our data center ensures both the physical security and consistent availability of your Wurk data and applications. As a result of these efforts, Wurk uptime has historically measured 99.79 percent or greater monthly for unscheduled outages. Our data center is designed to eliminate any single point of failure within the system architecture, provides the following features to maximize uptime:

- 24x7x365 monitoring of system operations
- N + N power redundancy
- Connectivity to multiple backbone providers
- Variable switch load technology
- Hardened operating systems on all servers

Uptime Architecture

The Wurk database availability strategy relies on SQL Server transaction log shipping to maintain copies of its production database on three different servers. This strategy helps ensure that your data, application configurations, and stored code continue to be available even if a server, SAN, or site experiences failure. The primary SQL database solution consists of two databases built in a cluster to provide instant redundancy in the event that one server fails. Transaction logs are shipped to another SQL Server in the production environment, thereby creating a local backup SQL server. Transaction log files are also shipped

via a secure transmission to an off-site SQL server at the disaster recovery location. Full database backup is performed weekly — with incremental backups running daily — to further minimize risk.

System Update Frequency

Our platform, Kronos®, applies regular system updates:

• **Service Packs**: Weekly — updates typically occur on Wednesdays

• **System Releases**: Monthly — updates typically occur on Thursdays

• **System Maintenanc**e: 24-hour notice — updates typically occur during the weekend

Data Center Uptime Facilities

The HVAC system maintains a consistent operating temperature and is powered by multiple 20-ton computer room air conditioning units and three 100-ton chillers. Redundant power lines provide over 265 watts of power per square foot utilizing two-megawatt transformers. If a power outage occurs, a two-megawatt Caterpillar diesel generator provides full load in less than 10 seconds and can run for more than 24 hours without refueling. Time-guaranteed contracts with multiple diesel fuel suppliers help ensure uninterrupted service.

Disaster Recovery Data Center

Because the data center stores and processes a wide range of human resources data, including confidential employee information, it is critical that the system is both highly available and highly secure. To this end, a multilayer availability strategy is applied across the Wurk cloud hosting infrastructure. Its cloud computing environment features a high availability design that helps ensure ongoing operation and proper functioning of the system even if individual components fail. To maintain business continuity in the unlikely event that our primary hosting site experiences a catastrophic failure, an emergency secondary data center is ready to take over production duties within a reasonable timeframe:

• **Recovery Point Objective** (RPO): 15 minutes

• **Recovery Time Objective** (RTO): 48 hours

The disaster recovery data center has all the space, power, and security features required for reliable, high-performance hosting and management of your Wurk solution. If you have any additional questions, you can always contact Support.