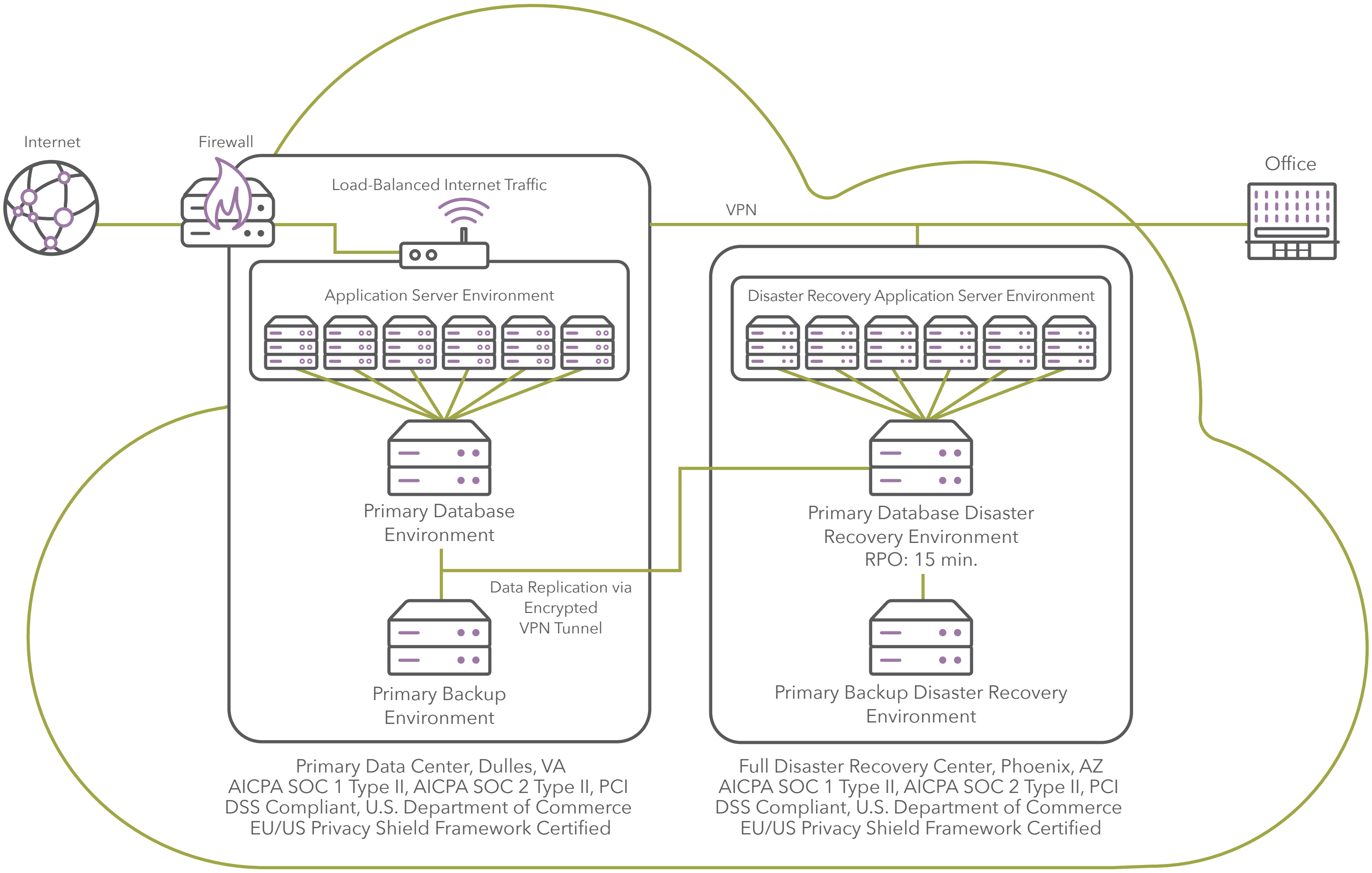
würk

World-Class Infrastructure, Security & Support for Cannabis Businesses

INTRODUCTION

Our human capital management (HCM) solution is a full-suite cloud solution that helps you manage your entire workforce from prehire to retire. Its comprehensive tool set integrates HR, payroll, recruiting, benefits administration, workforce management, and more so that you can manage and nurture your organization's most valuable asset, while giving managers single-source access to real-time employee data for engaging employees, attracting top talent, and making more informed business decisions. Offered exclusively as software as a service (SaaS), any module in our solution can be used individually, as part of a complete, integrated solution, or in conjunction with other third-party applications, content, and/or services. Our solution is offered through a single HCM application that is available to customers at any time, from anywhere.

The cloud-based solution is the ideal choice for organizations looking to achieve their HCM goals without exceeding their capital equipment budget or placing additional demands on their busy in-house IT staff. Because our solution is hosted in the cloud, you get 24*7 access to your solution without having to purchase additional hardware, operating systems, or database licenses. You gain peace of mind knowing that experienced technical consultants are managing the solution infrastructure, as well as your applications and employee data, to help ensure high availability, reliable performance, and multilayer 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 optimal results.


Internet
Firewall
Load-Balanced Internet Traffic
VPN
Office
Application Server Environment
Disaster Recovery Application Server Environment
Primary Database Environment
Primary Database Disaster Recovery Environment RPO: 15 min.
Data Replication via Encrypted VPN Tunnel
Primary Backup Environment
Primary Backup Disaster Recovery Environment
Primary Data Center, Dulles, VA AICPA SOC 1 Type II, AICPA SOC 2 Type II, PCI DSS Compliant, U.S. Department of Commerce EU/US Privacy Shield Framework Certified
Full Disaster Recovery Center, Phoenix, AZ AICPA SOC 1 Type II, AICPA SOC 2 Type II, PCI DSS Compliant, U.S. Department of Commerce EU/US Privacy Shield Framework Certified

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. This document describes the world-class infrastructure, services, processes, and policies behind our solution that enable us to deliver the availability, performance, and security your organization demands.

ARCHITECTURE/SYSTEM DESIGN

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 our solution's cloud infrastructure environment features a true multitenant architecture that 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 applications and 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 HCM that drives competitive advantage and bottom-line results.

Primary data center

Our solution is hosted at a secure off-site data center in Dulles, Virginia.* This world-class data center facility delivers cloud, managed hosting, and colocation services while providing superior integrated hosting services, carrier/network connectivity, and 24*7 security. This data center specializes in meeting industry-specific compliance standards to help ensure the ongoing security and integrity of your deployed solution. The primary data center is constructed and equipped to meet the most stringent security mandates for comprehensive physical, network, and policy-based security.

*Physical specifications for the primary data center are listed in Appendix A.

Security and auditing

The solution's environment has achieved the American Institute of Certified Public Accountants (AICPA) 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. Our solution provider has certified its compliance with the EU/US Privacy Shield Framework.

System uptime

The solution's developer works closely with the data center to help ensure both the physical security and consistent availability of your data and applications. As a result of these efforts, our solution's uptime has historically measured 99.79 percent or greater monthly for unscheduled outages.

The solution's data center facility, which is designed to eliminate any single point of failure within the system architecture, provides the following features to maximize uptime:

- 24*7*365 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 solution's database availability strategy relies on SQL Server transaction log shipping to maintain copies of its production database on two different servers. This strategy helps ensure that your data, application customizations, 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 one server fails. Transaction log files are shipped via a secure transmission to an off-site SQL Server cluster, also consisting of two servers that provide instant redundancy, at the solution's disaster recovery location.

Full database backup is performed weekly – with incremental backups running daily – to further minimize risk.

System update communications

The solution's Global Support will send system administrators a notification for all system updates. These notifications will also be posted in customer portal.

- Service Packs: Weekly – updates typically occur on Wednesdays
- System Releases: Bimonthly – updates typically occur on Thursdays
- System Maintenance: 24-hour notice – updates typically occur during the weekend

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

Because our solutions store and process 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, the solution's developer has implemented a multilayer availability strategy across its cloud-hosting infrastructure.

The solution's 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 the primary hosting site experiences a catastrophic failure, an emergency secondary data center in Phoenix, Arizona,* is ready to take over production duties within a reasonable time frame:

- Recovery Point Objective (RPO): 15 minutes
- Recovery Time Objective (RTO): 48 hours

The Phoenix-based disaster recovery data center has all the space, power, and security features required for reliable, high-performance hosting and management of your solution.

*Physical facility specifications for the disaster recovery data center are listed in Appendix B.

SECURITY POLICIES AND PROCESSES

Data security is a top priority for us. The solution developer's corporate security officer is the designated management representative responsible for implementing policies and procedures designed to protect and safeguard customers' workforce data.

Data collection and encryption options

Your organization's users access the solution's cloud environment from a web browser or mobile device via encrypted Transport Layer Security (TLS) sessions using port 443. Kronos InTouch® terminal connections are Ethernet-based using port 80 or 443. They can utilize TLS to encrypt data transmission when you provide a digital ID certificate from a third-party vendor. Data at rest is encrypted across the system's environment by utilizing Transparent Data Encryption.

Secure system login

Solution end-users authenticate using a unique password. Our solution uses industry-standard, modern hashing algorithms to secure these passwords, and they are never stored in clear text.

Your end-users may gain access to the solution via Single Sign-On (SSO). To implement Security Assertion Markup Language (SAML) 2.0, Our solution requires an X.509 certificate, which may be self-signed. You will also need to provide the entity ID of your Identity Provider, such as ADFS 2.0, and a login redirect URL. Once a user is logged in via SSO, a multifaceted security profile controls the role-based functional and data access rights of supervisors and employees.

Browser support

End-users may access the solution's applications via a web browser or mobile app provided the following requirements are met:

- Internet Explorer®: Versions 10 or 11
- Edge
- Chrome™/Firefox®/Safari®: Current versions
- Mobile: We have limited support for mobile platforms using the browsers listed above

Mobile app support

The solution's mobile app runs on the following Apple or Android mobile devices with a data plan or Wi-Fi:

- Apple® iOS: Latest versions
- Android™ OS: 5.0 and higher

Physical and logical security features

The solution is hosted and managed in a private cloud deployed from an AICPA AT101 SOC2-compliant data center with multilevel physical and logical security features, including:

- **Intrusion Prevention System (IPS)/Intrusion Detection System (IDS):** Our solution deploys next-generation firewalls, which restrict network traffic to authorized traffic.
- **Secure Transmission Sessions:** Secure protocol versions TLS 1.2 and above are supported.
- **Virtual Code Authentication:** Our solution requires virtual code authentication – user name, password, and a system-generated code. Passwords are required to be complex with a minimum number of characters and expiration at a predefined interval. (See Virtual Code Authentication datasheet for more information.)

- **Best-Practice Coding:** Our solution developer employs secure coding practices and control processes across application development and software maintenance. Code reviews are conducted regularly to identify potential security flaws.
- **Penetration Testing:** Our solution developer uses a qualified third-party vendor to perform penetration testing annually.
- **Vulnerability Scanning:** Our solution developer conducts vulnerability scanning using a third-party tool, evaluates identified risks, and develops remediation and/or mitigation plans to address the vulnerability.
- **Antivirus Software:** Our solution developer deploys a third-party, commercially available antivirus solution on servers to prevent viruses and malware from being deployed in the cloud environment.
- **Patch Management:** Our solution developer patches the system's environment regularly as a routine part of maintaining a secure cloud infrastructure. Patches are reviewed by the solution's engineers as they are released from the vendors. Approved patches are tested and then deployed to the environment in accordance with change management policies.
- **Risk Assessment:** Our solution developer conducts an annual risk assessment of the solution's cloud environment to determine whether the control framework achieves the data privacy and data security objectives.
- **Security Incident Management:** Our solution developer maintains an escalation procedure to notify appropriate management staff and customer contacts in the event of a security incident. The event is worked to resolution and a root-cause analysis is performed.

Security and data protection training

Our solution developer conducts Security and Data Protection Awareness Training for new and existing employees. New employees are required to complete training within 60 days of their date of hire and annually thereafter. This training focuses on teaching employees what information constitutes personal information, how to protect confidential data and personal information, and security trends of which its employees need to be aware. At the conclusion of the training session, employees must pass a test to demonstrate their understanding of data protection and security and privacy awareness issues.

Background checks

Before extending an offer of employment to a candidate, our solution developer conducts background checks to determine whether he or she is eligible for hire. These checks include education and employment history verification, and if permitted by law and authorized for the position in question, criminal background and credit check searches.

Certifications

The solution developer's Cloud Services team has the breadth and depth of IT experience, technical skills, and application expertise required to manage, support, and maintain your cloud-hosted HCM system. Its team members have earned a wide range of technical and security certifications, which prove they have amassed the experience and mastered the skills needed to deliver reliable, high-performance cloud-hosting services. These certifications include:

- Microsoft® Certified Professional
- Microsoft Certified Technology Specialist (MCTS)
- Microsoft Certified Solution Developer (MCSD)
- PMI's Project Management Professional (PMP)®
- ITIL v3 (Foundation)
- CompTIA A+ (2008), Computer-Communications Systems Supervisor – 7 level (military)
- Microsoft Certified Professional (MCP Server 2003)

- Microsoft Certified System Administrator (MCSA Server 2003)
- Microsoft Certified Technology Specialist (MCTS SQL 2005)
- Juniper Certified – JNCIA-EX (Associate, Enterprise Switching)
- Juniper Certified – JNCIS-ER (Specialist, Enterprise Routing)
- Microsoft Certified DBA (MCDBA)
- VMware® Certification
- HP® 3Par Storage Certification
- HP Data Protector Certification
- Certified Information Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

CHANGE MANAGEMENT

Our solution developer has established a formal change management process to guide the request, development, testing, approval, and implementation of changes, including emergency changes, to the solution's environment. This process differentiates among infrastructure changes, application changes, and customer-specific configuration changes, each of which is handled according to a specific set of predefined steps.

When a change is needed to the solution's environment, the change requestor — typically a member of the Cloud Services team — completes a change request that includes the type of change, priority, description, test plan, deployment instructions, back-out plan, validation plan, customer impact, and risk assessment. The type of change and its priority determine which approvals are needed to proceed. Upon approval, the change request is authorized to move through the change management process and into production during scheduled maintenance windows on Wednesdays from 12:01 – 4 a.m. and on Saturdays from 12:01 – 6 a.m.

Code changes to the solution's environment follow a standard System Development Lifecycle (SDLC). Our solution developer uses an Agile development methodology with monthly sprints. At the end of each sprint, it deploys a new system release during a scheduled maintenance window. Code changes must be approved for development and undergo quality assurance testing before being deployed in production. All steps in the SDLC process are documented in a ticket.

SYSTEM INTEGRATION

Integrating existing applications with your HCM solution is critical to a successful implementation. Integration Hub, part of our HCM solution suite, speeds and simplifies integrations between our solution and any combination of cloud, SaaS, or on-premises applications. It allows integrations between our HCM solution and third-party systems – using industry-proven integration tools – quickly and efficiently, for improved data integrity and faster time to value.

We will assess your unique requirements and determine the best integration strategy to meet your needs. Our experts will use one or more of the following technologies (included in Integration Hub) to build and deploy your integrations:

- **Middleware:** This integration option may be used to connect our solution applications to on-premises legacy systems, thereby enabling you to send files to a local network printer, upload files from a local network to the cloud, or download files from the cloud to a local computer. Our experts may also use middleware to automate the upload of information – employee data, accrual balances, cost centers, time punches, and more – from your local network to central servers.
- **REST APIs:** The REST architecture, used by technology leaders such as Google, Yahoo, Amazon, and Twitter, is now a common standard for achieving integration across systems through a series of bidirectional APIs. Working as an underlying layer for data access, the REST architecture provides public XML APIs – wrapped in a web service – which are generally executed using GET and POST commands. Our solution hosts a robust library of REST APIs, which it continues to expand with each product update.
- **Import/export:** Import templates, available for various functionality and settings, allow customers to import data directly into our solution. Authorized users simply select the template style for the desired import type, such as an Excel version of an employee import, benefit plans, payroll history, employee skills or work preferences, or time-off requests from other systems. System data export allows authorized users to define the information and file-naming convention used for a data export file. They can also export custom forms by selecting the file format desired for the data export file, such as CSV, Fixed Width, and Custom Settings, and configuring the data export file as needed. Standard export files include payroll exports, benefit plans, training, certifications, and more.

APPENDIX A

Primary Data Center Specifications

Square Footage	• Leased: 64,000 sq. ft. • Colocation Area: 30,821 sq. ft. • Flex Space: N/A • Satellite Platform: 1,000 sq. ft.
TELCO Information	• NPA/NXX: 703-840 • CLLI Code: ASBNVAAS • LEC: VERIZON • LATA: 246
Cooling	• Cooling Capacity: 4 kW per cabinet (higher densities available) • Cooling Plant: Air-cooled RTUs with adiabatic humidification
Power	• Electrical Capacity: 4 kVA per cabinet (higher densities available) • UPS Configuration: N+1, Block Redundant System • Number of Utility Feeders: 1 • Number of Power Transformers: 3 • Utility Voltage: 34.5 kV, 3-phase • Standby Power: 4-3,000 kW diesel engine-generator power • Standby Power Configuration: N+1, Block Redundant
Security	• Physical: "Man trap" entry; perimeter fencing • Human: 24*7 armed security guards • Electronic: CCTV and recorders; motion detection; biometric readers; fiber vault
Building	• Construction Type: 2C Unprotected • Building Type: Two story, precast concrete slab on grade • Floor Load Capacity: 175 PSF
Building Code Compliance	• Building: 2009 Virginia State Building Code (VSBC) • Mechanical: 2009 International Mechanical Code • Plumbing: International Plumbing Code • Electrical: 2008 National Electric Code • Life Safety: 2009 NFPA 13: Installation of Sprinkler Systems; 2009 NFPA 72: National Fire Alarm Code • Sprinkler Systems: 2009 NFPA 72: National Fire Alarm Code • Other: ADA Guidelines
Lateral Load Design	• Seismic EPV(Av): Av = 0.05 • Seismic EPA(Aa): Aa = 0.05 • Seismic Hazard Exposure: Site Class C • Seismic Importance Factor Ie: N/A • Seismic Zone: 1 • Wind Exposure: 90 mph basic wind speed • Wind Importance Factor: Iw = 1.15
Fire Protection	• Fire Suppression: Double-interlocked, pre-action (dry pipe) • Fire Rating: Minimum 1-hour rating
Interconnection Options	• System: Overhead proprietary cable tray system with multitier ladder rack • Cross Connects available: Single-Mode fiber, Multi-Mode fiber (62.5 and 50 micron), CAT5, CAT6, CAT5 (T1), and CAT3 (POTS) • Intra-Building Innerduct (IBID) available: a dedicated private path via a conduit between buildings or customers – Each private path innerduct is 1.25" in width – Customers run their own single-mode fiber within the innerduct, which can potentially fit 432 standard cross connects • Equinix Exchange™ available: Central switch for public and private peering

APPENDIX B

Disaster Recovery Center Specifications

Physical Building	• Three-story building with 380,450 total sq. ft. • 108,000 sq. ft. of raised floor, 10,787 sq. ft. of meeting space ("Meet-Me Room") – premier internet gateway facility for the area • Built-up roof system • Outside 500-year floodplain • Floor loading varies from 100 to 400 PSF • Clearance height varies from 10 ft. to 15 ft. • 24*7 security staff with card key biometric access control, digital video monitoring and recording, and diverse underground conduit entry vaults
Secondary Power	• 17 generator positions; nine generators of various sizes installed and eight sited and available • Multiple bulk diesel fuel storage tanks with 10,500 gal. of diesel storage and 80,000 gal. permitted and sited • Ample space for tenant generators, fuel storage, and UPS power
Cooling/HVAC	• Two 1,000-ton cooling towers with an additional 1,000-ton cooling tower sited • Ample space for tenant equipment
Fire Protection	• Double interlock pre-action fuel vaults with foam suppression • VESDA