COMPLETE PAYROLL SOLUTIONS

Technical Paper

Workforce Management Solutions:

World-Class Infrastructure, Security, and Support for the Experience You Expect

866-658-8800

CompleteWorkforce

KRONOS AUTHORIZED partner

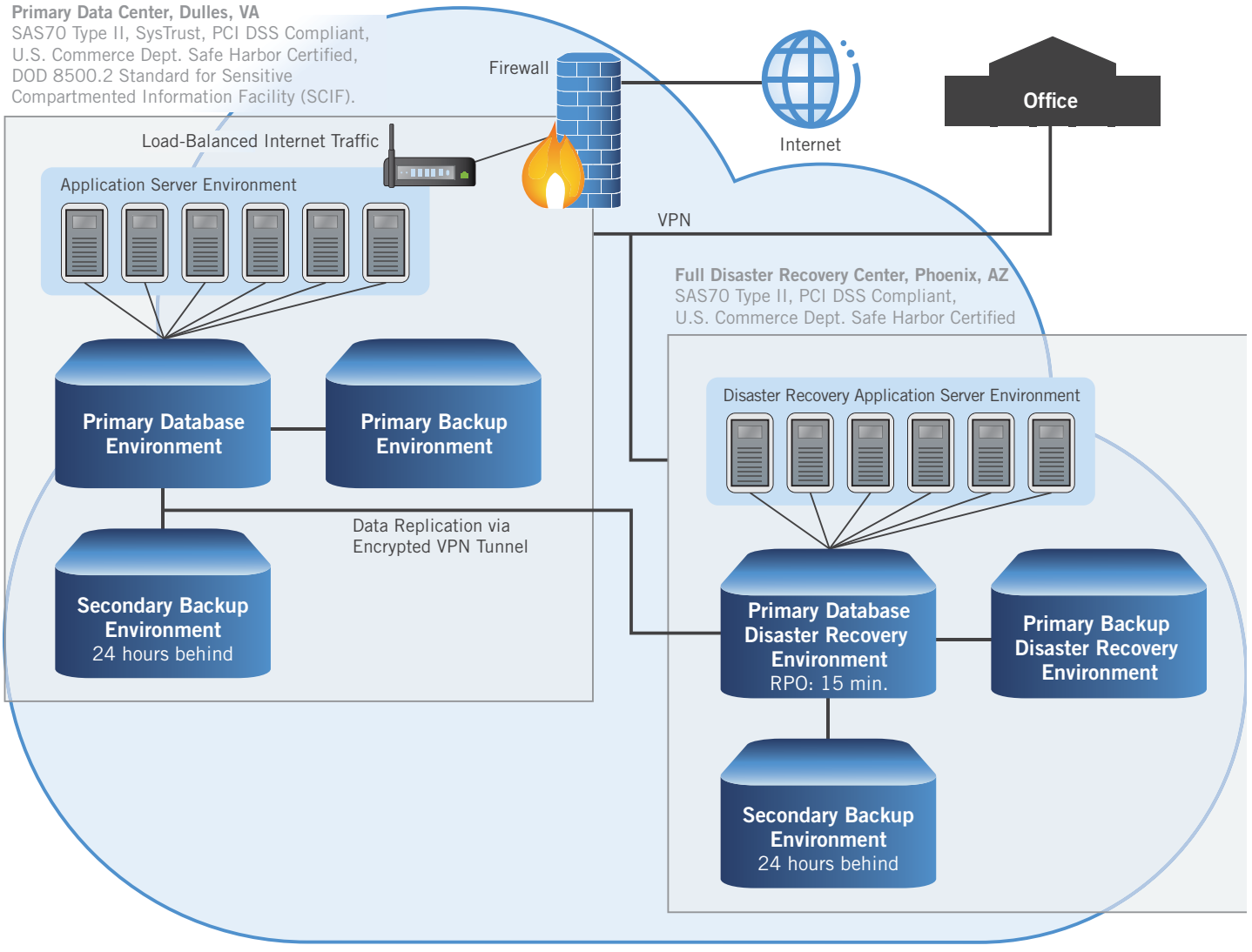
TABLE OF CONTENTS

INTRODUCTION

A workforce management solution helps organizations like yours control labor costs, minimize compliance risk, and improve workforce productivity. Offered exclusively as Software-as-a-Service (SaaS), the solution offers applications for human resources (HR), payroll, time and attendance, leave, accruals, scheduling, and more. Each application can be used individually, as part of a complete, integrated solution, or in conjunction with other third-party applications, content, and/or services. The workforce management solution delivers a single front-end interface that is available to customers at any time, from anywhere.

The cloud-based solution is the ideal choice for organizations looking to achieve their workforce management goals without exceeding their capital equipment budget or placing additional demands on their busy in-house IT staff. Because the workforce management solution is hosted in the cloud, you get 24x7 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 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 optimal results.

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 workforce management solution. This document is intended to describe the world-class infrastructure, services, processes, and policies behind the workforce management solution that enable us to deliver the availability, performance, and security your organization demands.



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 this workforce management solution's cloud infrastructure environment features a true multi-tenant 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 workforce management 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 workforce management that drives competitive advantage and bottom-line results.

PRIMARY DATA CENTER

The workforce management 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 24x7 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 workforce management solution environment 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. The environment is Safe Harbor Certified.

SYSTEM UPTIME

We work 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, the system's uptime has historically measured 99.5 percent or greater monthly.

The data center facility, which 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 platform 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 UPDATES

All updates occur on Wednesdays or Thursdays at midnight, U.S. Eastern time.

- Service Packs: Weekly
- System Releases: Monthly
- System Maintenance: 24-hour notice

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 workforce management 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, a multi-layer availability strategy has been implemented across the solution's cloud hosting infrastructure.

The 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 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 workforce management 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. We have a 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 platform'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.

SECURE SYSTEM LOGIN

End-users authenticate using a unique password. Industry-standard, modern hashing algorithms are used to secure these passwords, and they are never stored in clear text.

Your end-users may gain access to the workforce management platform via single sign-on (SSO). To implement security assertion markup language (SAML) 2.0, the platform 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 multi-faceted security profile controls the role-based functional and data access rights of supervisors and employees.

BROWSER SUPPORT

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

- Internet Explorer®: Versions 9, 10, or 11
- Chrome™/Firefox®/Safari®: Current versions
- Mobile: We have limited support for mobile platforms using the browsers listed above

MOBILE APP SUPPORT

The mobile app runs on the following Apple®, Android™, or Windows® Mobile devices with a data plan or Wi-Fi:

- Apple iPhone® or iPad® with iOS 4 or higher
- Android OS 2.2 or higher
- Windows Mobile OS

PHYSICAL AND LOGICAL SECURITY FEATURES

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

- **Intrusion Prevention System (IPS)/Intrusion Detection System (IDS):** Next-generation functionality firewalls are deployed, which restrict network traffic to authorized traffic.
- **Secure Transmission Sessions:** Secure protocol versions TLS 1.1 and above are supported.
- **Virtual Code Authentication:** The workforce management 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:** 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:** Uses a qualified third-party vendor to perform penetration testing annually.
- **Vulnerability Scanning:** Conducts vulnerability scanning using a third-party tool, evaluates identified risks, and develops remediation and/or mitigation plans to address the vulnerability.
- **Antivirus Software:** Deploys a third-party, commercially available antivirus solution on servers to prevent viruses and malware from being deployed in the cloud environment.
- **Patch Management:** Patches the workforce management solution environment regularly as a routine part of maintaining a secure cloud infrastructure. Patches are reviewed by 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:** Conducts an annual risk assessment of the workforce management solution cloud environment to determine if the control framework achieves the data privacy and data security objectives.
- **Security Incident Management:** 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

Security and data protection awareness training for new and existing employees is conducted. 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 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, background checks are conducted to determine if 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 Cloud Services team has the breadth and depth of IT experience, technical skills, and workforce management application expertise required to manage, support, and maintain your cloud-hosted workforce management system. 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 Solutions 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 Systems 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

A formal change management process has been established to guide the request, development, testing, approval, and implementation of changes, including emergency changes, to the workforce management system'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 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 to 4:00 a.m. and on Saturdays from 12:01 to 6:00 a.m.

Code changes to the workforce management solution environment follow a standard system development lifecycle (SDLC). The platform uses an Agile development methodology with monthly sprints. At the end of each sprint, a new release is deployed 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

SYSTEM INTERFACES

In order to take full advantage of the workforce management solution, interfaces are used to import and export data to and from the system. All interfaces use the flat file transfer method to move data between systems. Several interfaces may be needed between the platform and other HR/payroll applications. Some interfaces will be recurring and some will only be used once to populate the system. The intended purpose of an interface is to keep all systems in sync. Your consultant will work with you to determine the frequency of the interface export/import process.

MIDDLEWARE

The workforce management solution cloud environment uses a middleware application that automates the upload and download of information, including employee data, accrual balances, cost centers, punches, and payroll data, from your network to the cloud environment. The middleware can be pointed to a specific directory on your local server or network to retrieve a file for automatic upload to the cloud. It can also deposit a file from the cloud environment to a specified directory on your local server or network. The middleware connects to the workforce management solution in the cloud via an HTTPS connection at predefined intervals.

Middleware is a Java application that requires implementation of the Java runtime environment version 1.6 or higher within your local network environment.

CLOUD SERVICES

SUPPORT

As the leader in workforce management, we offer support services to help you get the experience you expect. Our support services provide access to valuable tools and information to help you diagnose and resolve issues quickly and efficiently in order to optimize productivity and realize continuous value from your investment. When our self-help tools aren't enough, our skilled, knowledgeable support professionals — with 5-10 years of domain experience on average — are ready to put their expertise to work for you.

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: 4kW per cabinet (higher densities available) • Cooling Plant: Air-cooled, RTUs with adiabatic humidification
Power	• Electrical Capacity: 4kVA 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: 24x7 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 multi-tier 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 Cloud Exchange™ Available: Central switch for public and private peering

APPENDIX B

Disaster Recovery Center Specifications

Physical Building	• Three-story building with 380,450 total square feet • 108,000 square feet of raised floor, 10,787 square feet of meeting space (“Meet-Me Room”) — premier internet gateway facility for the area • Built-up roof system • Outside 500-year flood plain • Floor loading varies from 100 to 400 lbs./square foot • Clearance height varies from 10 feet to 15 feet • 24x7 security staff with card key biometric access control, digital video monitoring and recording, and diverse underground conduit entry vaults
Secondary Power	• 17 generator positions; 9 generators of various sizes installed and 8 sited and available • Multiple bulk diesel fuel storage tanks with 10,500 gallons of diesel storage and 80,000 gallons 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

KRONOS AUTHORIZED partner