

# Cloud Delivery

Enhanced security. Greater accessibility. The confidence that your system is always up to date. These are just a few of the reasons why more organisations are moving their technology solutions to the cloud. As you weigh your organisation's options, look to WFS: A WorkForce Software Company (WFS Australia®) as your partner for enterprise workforce management. Our cloud package delivers:

- **Unmatched value** – A low predictable recurring, per-employee subscription fee covers all your software, hardware, maintenance, and support
- **More immediate returns** – A quicker deployment maximises the return on your organisation's investment
- **Rigorous controls** – SSAE 16 Type II, ISAE 3402 Type II, SOC 2 Type II, and U.S.-EU Safe Harbor and/or EU-U.S. Privacy Shield annual audits ensure strict security controls and procedures
- **Smooth updates** – Three seamless updates per year minimise disruption and allow your business to stay current
- **Perpetual innovation** – Immediate access to new features keeps your business at the forefront of workforce management best practices
- **Anywhere access** – Pure web-based design gives your workers greater freedom in how they complete timely self-service tasks.



Our cloud infrastructure has met the stringent standards of some of the world's leading organisations, who rely on our WFS Suite to automate workforce management across business lines and national borders. Hosted in world-class data centres around the globe and managed by our SaaS experts, cloud delivery offers all the workforce management tools you need, with none of the overhead.

## Keeping Your System—and Data—Secure

In choosing a cloud provider, there is nothing more critical than security, particularly when it comes to protecting employee data. That's why we've invested heavily in our cloud infrastructure and auditing procedures to make sure that we continually meet—and often exceed—the highest standards for security, reliability, and performance. Selected highlights of our security measures include:

### Physical Security

Each of our global SaaS facilities require a key card, PIN and/or biometrics to enter, and are monitored 24x7 with video surveillance. Each facility has redundant power and air conditioning systems, and generators with at least 24 hours of fuel and Priority 1 refueling (the same priority as hospitals and police). All equipment runs within locked cages and/or cabinets. WFS Australia owns, maintains, and supports all equipment and applications.

## Perimeter Security

DDoS services protect against Distributed Denial of Service attacks, while firewalls protect secure traffic from the Internet and regulate traffic between key subnets. Intrusion detection systems continuously monitor the SaaS environment.

We perform routine internal and external vulnerability scans, and contract with third-party security firms to perform independent vulnerability scans, annual penetration tests, and annual web application security tests. WFS Australia proactively analyses security logs to identify security threats.

## Data Encryption

The WFS Suite SaaS platform support the strongest HTTPS (TLS) encryption supported by your organisation's browsers. Data from clock terminals is encrypted over the Internet, and secure protocols are used for bulk file transfers. Data at rest, including backups, are encrypted with AES-256 encryption.

## User Authentication

Clients can customise password rules within WFS Suite's native authentication systems, and/or use LDAP or Single Sign-On (SSO) to authenticate against your directory services.

## Database Security

Database access is strictly controlled and monitored. Database access is audited monthly.

## Internal System Security

We use non-routable IP addressing, port-redirection, network address translation and other mechanisms to protect systems within the firewalls. All servers are hardened by disabling or removing unneeded services and protocols. Systems are routinely patched for security.

## Redundancy and Disaster Recovery

All network components, load balancers, proxy servers, application servers and database servers have redundant hardware. WFS Australia has multiple redundant Internet providers. We maintain complete disaster recovery facilities with duplicate hardware, software and Internet connectivity. Your data is replicated to standby servers at both the Primary Site and the Disaster Recovery Site.

## Backups and Restores

We perform full database backups weekly and incremental backups daily, and we store these encrypted backups at both our Primary and Failover SaaS Sites. Routine restore tests verify that backed-up data is accessible.

## Operating Procedures

WFS Australia adheres to documented Change Management Procedures. All changes require approval from the Change Approval Board. Access to the SaaS environment is strictly limited, and access must be approved in advance by our Change Approval Board.

### Bringing It All Together

With deep knowledge of industry best practices and a collaborative, client-centred approach, WFS: A WorkForce Software Company is one of the fastest-growing and most trusted cloud providers. And we're here to partner with you to accomplish all of your workforce management goals—down to the most complex challenges you face.

### How Can We Help You?

Give us a call at **61 2 8399 1688** to speak with an expert about moving your workforce management solution to the cloud or visit us at **wfsaustralia.com** to request a personalised demonstration.