



# Departmentware

## External Security Statement

Document Version: 1.7.4  
Data Classification: Public  
Updated July 1, 2026

|                                                      |          |
|------------------------------------------------------|----------|
| <b>Overview.....</b>                                 | <b>3</b> |
| <b>Security Summary.....</b>                         | <b>3</b> |
| <b>Architecture.....</b>                             | <b>3</b> |
| <b>Account Management.....</b>                       | <b>4</b> |
| <b>Compliance &amp; Infrastructure.....</b>          | <b>4</b> |
| <b>Communication &amp; Operations.....</b>           | <b>4</b> |
| <b>Application Security.....</b>                     | <b>5</b> |
| <b>Authentication.....</b>                           | <b>5</b> |
| <b>Vulnerability Management.....</b>                 | <b>5</b> |
| <b>Information security incident management.....</b> | <b>5</b> |
| <b>Business Continuity and Recovery.....</b>         | <b>5</b> |

## Overview

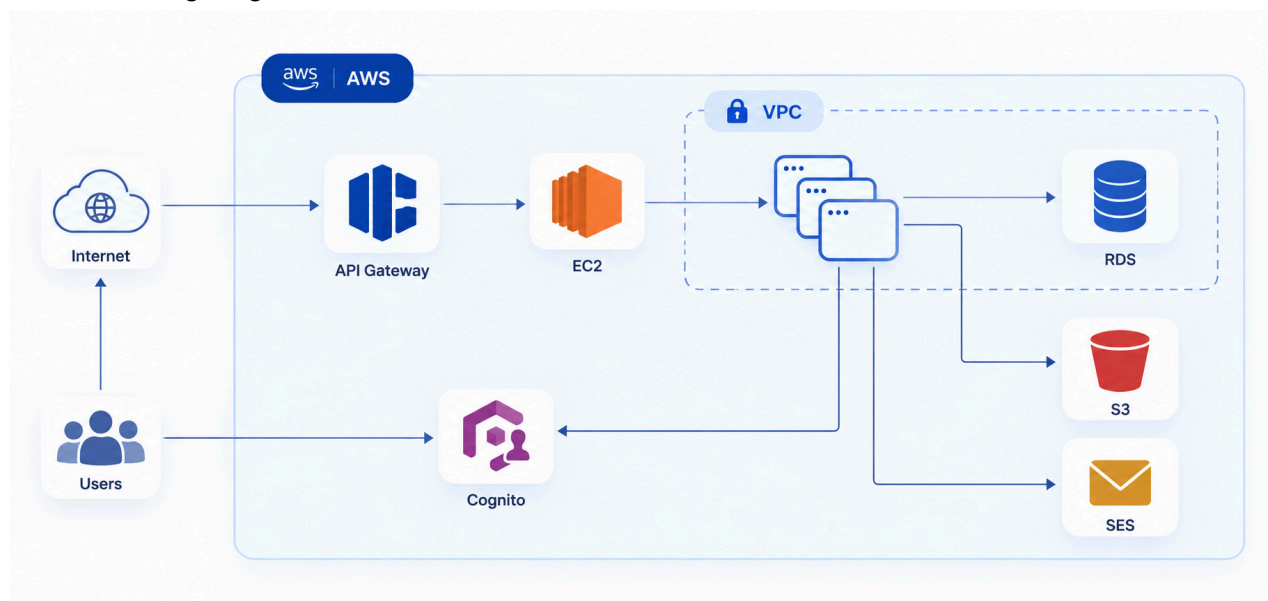
- Departmentware, Inc. ("DW") is a customizable Software-as-a-Service compliance platform for public safety that addresses onboarding of new officers and lateral hires and is aligned with programs commonly referred to as FTO and PTO.
- Departmentware cloud services are hosted and delivered by Amazon Web Services ("AWS"). Amazon is responsible for the security of its actual data centers and the AWS cloud. DW is responsible for monitoring, managing and securing the DW application and data. We take security seriously and protect your data as described in detail below.
- All DW customer data and infrastructure resides within the continental United States ("US") with redundant server resources positioned on the east and west coasts of the US. Our policies require quarterly vulnerability audits and monthly patch cycles.
- Customer data is encrypted end-to-end and DW follows industry standards and AWS' recommendations for secure data handling.

## Security Summary

- Security is a key priority for Departmentware, Inc. We maintain information security incident management processes that prioritize, fix and communicate via a documented workflow.
- Security policies are reviewed annually and tested monthly.
- All infrastructure and customer data is hosted on US infrastructure.
- All customer data is fully encrypted end-to-end from the database to delivery within a web browser.
- Access to DW infrastructure is managed by a very limited number of individuals whose access is monitored quarterly by the principals of the business.

## Architecture

- Table of technologies (Phoenix - Application Server, React/Javascript - Front-end, PostgreSQL - database, SSL, ELB - Elastic Load Balancing)
- Hosting diagram



- *Fault tolerance/redundancy*
  - *Multiple compute instances running in different availability zone behind a load balance*
  - *7 days database backup*
  - *Ready to go database instance in another availability zone*

## Account Management

- DW manages and controls access to DW infrastructure
  - DW's business principals grant and monitor access to DW infrastructure
  - DW's business principals grant and monitor access to DW customer accounts
    - Inactive accounts are disabled on a periodic basis.
  - Within the DW application, DW customers have an administrative interface, limited to customer-defined users, to create system accounts to use the DW application
  - DW customers manage access to their system independently via an administrative system functionality assigned to a limited set of customer-defined users.
- All customer data is classified based on the type of data stored and appropriate application and infrastructure controls are applied consistent with industry standards.

## Compliance & Infrastructure

- Reference this page for a detailed overview of security and compliance measures employed by AWS: <https://aws.amazon.com/compliance/programs/>

## Communication & Operations

- DW will notify clients via email if the product is unavailable within 2 hours
- DW support operations are available seven days a week - 7AM-8PM CST including holidays.
- DW change management processes include a risk assessment of new code, testing, and a communication plan to share changes with customers.
- DW system capacity management - monthly review of capacity and performance. DW responsible for ensuring that systems are responsive.
- DW data management - Encryption at rest, TLS using 2048 bit key. Resilience and availability by utilizing Platform-as-a-Service technology and multiple data centers.

## Application Security

- DW maintains system logs to audit system faults and login history.
- User activities and system administration activities are logged.
- DW utilizes software to review and notify when suspicious/anomalous activity is detected.

## Authentication

- DW business principals sets up accounts during onboarding of customers
- Customer administrators disable system accounts at their discretion
- DW periodically reviews logins history to disable idle accounts
- Customers are responsible for identifying administrative users at their department

- All changes are captured in audit log
- Built-in account validation process includes automated email link to ensure only secured users can access the system.

## **Vulnerability Management**

- DW monitors for significant vulnerabilities in the application and infrastructure
- DW performs monthly patching and out-of-schedule patching for urgent issues
- DW uses vulnerability scanners to access and monitor DW environments

## **Information security incident management**

- DW has documented roles and procedures for handling security incidents.
- Summary of key workflow steps
  - Create incident
  - Identify key stakeholders
  - Investigate within four hours
  - Identify root cause
  - Remediate
  - Communicate
  - Amend internal procedures if DW identifies an internal deficiency
- Formal risk mitigation procedures may include conducting an investigation, where appropriate, disclosing a breach to interested parties including regulators and law enforcement authorities.

## **Business Continuity and Recovery**

- No technology is 100% immune from defects and outages
- DW understands the criticality of the application to your department and works to ensure our infrastructure is resilient and recoverable, minimizing single points of failure
- DW relies on industry leading AWS for security, uptime
- DW can architecture additional resilience for clients where financially feasible
- Recovery Time Objective is 48 hours