Supplier corporate IT

# Supplier corporate IT

The Ministry of Justice (MoJ) does **not** by default prohibit the use of supplier organisation corporate IT for the processing of MoJ data on the basis that the corporate IT environment is well designed, maintained, governed and defended in line with large scale commercial threat models.

Subject to the suitability described, the MoJ does **not** require suppliers to create or maintain dedicated or segregated IT solutions for the processing of MoJ data classified at OFFICIAL.

## Technical security

Supplier corporate IT systems are expected to maintain appropriate levels of technical security defences to proportionally defend all types of data within whether the supplier's own corporate data through to MoJ data being processed.

This will range (but not be limited to) the use of modern Transport Layer Security or IPSec for in-transit encryption through to modern hashing and cryptography mechanisms for data stored at-rest, whether a data entry in a database or the entire storage drive in a laptop.

Supplier systems are expected to be proportionally resilient to malware, ensuring segregation between systems, users and data and employ adequate commodity measures (such as email attachment scanning/filtering).

### Email security

Supplier corporate email systems processing MoJ data are expected to align to the [UK government secure email policy](https://www.gov.uk/guidance/securing-government-email) which summarily requires widely accepted best practices.

Supplier corporate email systems are *not* required to technically integrate to the Public Services Network (PSN).

## Data Governance

### Data offshoring

Supplier's may process MoJ data (including Personal Data for which the MoJ is responsible) outside of the United Kingdom, subject to the maintenance of adequate information controls and governance.

MoJ data must not routinely be processed within an incompatible legal framework to the United Kingdom.

#### Working abroad

Supplier staff are **not** prohibited from working abroad while processing MoJ data on the basis that adequate information controls and governance are maintained.

When working abroad, this may include limiting access to information while the user travels or using secondary temporary accounts to avoid primary account compromise.

### Data backups

Supplier corporate IT systems may backup data for extended retention times (for example, keeping archived or deleted emails for an additional few months). Backup systems may also exist in such a way that individual backup items cannot be individually deleted, and are subject to a system-wide backup rotation/retention schedule.

Subject to appropriate data governance, the MoJ acknowleges these cases.

### Local end-user device data

The MoJ acknowleges that corporate users typically 'download' files (from local email client caching to file downloads via a web browser) that can remain within 'Downloads' folders until explicitly deleted by the user.

MoJ expects suppliers to consider these types of data locations in data governance regimes, however it is appreciated that data destruction may be guidance based from the supplier organisation to supplier staff.