Compliance Statement

August 2026

Telephone: 01625 900 630 Email: info@ieg4.com
Enabling a Digital Society www.ieg4.com

IEG4 has received requests from a number of customers to confirm our status in relation to the "Memorandum of Understanding between the Department for Work and Pensions and local authorities" (MOU) and our role as a Contracted Service Provider as defined within the MOU.

Local authorities (LAs) are asked to "manage their suppliers to ensure they are compliant with all security and policy requirements within this MOU".

Within the MOU, there are recommendations that LAs:

- Establish and agree all relevant security requirements within contracts for their suppliers that process, store or transmit DWP, HMRC or Home Office Data

- Perform security due diligence and assessment on suppliers prior to on-boarding or processing DWP, HMRC or Home Office data.

We shall deal with each of these areas in turn.

Relevant Security and Process Requirements.

There are a number of obligations contained within the MOU which primarily fall within the remit of the LA to manage. However, there are also certain elements of our services which impact on compliance including:

a) Configuration and change management practices

IEG4 has configuration and change practices to manage the impact of service variations. Configuration management within IEG4 is implemented via a series of toolsets and procedures to ensure we manage the information on all relevant components that enable the provision and operation of the IEG4 digital platform. The Change enablement practice for IEG4 is primarily focussed on the delivery of software/platform changes but we do recognise that change can impact any configuration items and our practice embraces potential infrastructure changes.

b) Anti-malware

The IEG4 Azure Digital Platform operates a defence-in-depth malware protection approach aligned with the requirements of the DWP Security Standard SS-015 (Malware Protection). Malware protection is provided through Microsoft security technologies, including Microsoft Defender, together with Azure platform security

controls, network and application-layer protection and vulnerability and patch management processes. Anti-malware protection is centrally managed and maintained, with malware detection and security events centrally logged and monitored. Access to security configuration is restricted through role-based access controls and privileged access controls. Malware definitions, detection capabilities and security updates are maintained automatically, with detected threats subject to appropriate blocking, quarantine and remediation. These controls operate within IEG4's ISO/IEC 27001-certified Information Security Management System and provide layered protection against malware across the infrastructure.

c) Access Control

Access to LA data for LA staff is under the control of our customer. Access to LA data from within IEG4 is managed via role-based access control and applies the principle of least privilege access. IEG4 staff access to the database and other Azure services is restricted by role and Azure AD Privileged Identity Management (PIM). This ensures that staff only have the access they need to support the system and only at the time they need it. All elevated access is logged within the PIM service. Role elevation requires two-factor authentication.

d) Cyber resilience

Key features of the IEG4 information and cyber security management approach include that we:

- have appropriate information security and incident management policies
- ensure IEG4 staff are aware and regularly trained on security best practice
- limit access control with strict permission/approval-based functionality where IEG4 staff require access to databases/data
- encrypt all data at rest and in transit
- have disaster recovery/business continuity plans
- remove personal data from any places where it is not required e.g. reporting (this includes use of parameters to allow Councils to implement automatic removal of data in line with their GDPR polices).

We have adopted and implemented processes such that IEG4 security measures comply with all 14 principles of cloud security as defined by the National Cyber Security Centre (NCSC). Our current process and procedures are mapped to the NCSC 10 Steps to Cyber Security, and we are evaluating the recent Cyber Security Toolkit for Boards to help validate the robustness of our management processes in relation to Cyber Security.

IEG4 holds ISO27001 accreditation and is Cyber Essentials Plus (as well as basic) accredited, as well as compliant with the DSPT (Data Security and Protection Toolkit) requirements for the NHS.

e) Encryption requirements

IEG4 solutions provide for encryption of data both in transit and at rest.

Data transfer from a web browser to the back-end API is over HTTPS secured via TLS1.2. Within the Azure cloud data transfer from the backend API to Azure SQL and Azure Storage is over an encrypted channel. Integration models employ a variety of encryption and/or security mechanisms to ensure the data is protected and there is no data leakage e.g. data is posted to Council's back-office systems via Azure WCF Relay using encrypted keys and a Council-specific endpoint.

Data at rest protection is provided by security features offered through Azure. All data is stored in a combination of Azure SQL and Blob storage containers both of which have encryption at rest enabled.

TDE is used to encrypt SQL Server, Azure SQL Database, and Azure Synapse Analytics data files in real-time, using a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery.

TDE protects data and log files, using AES and Triple Data Encryption Standard (3DES) encryption algorithms. Encryption of the database file is performed at the page level. The pages in an encrypted database are encrypted before they are written to disk and are decrypted when they're read into memory.

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

f) Risk Management

IEG4 has a formal risk management policy and maintains a risk register, which forms an integral part of its management review process. A member of the Senior Leadership Team (SLT) has been appointed as the Data Protection Officer and is responsible for ensuring that appropriate operational and technical measures are in place to protect Local Authority (LA) data. The risk register is reviewed quarterly by both the SLT and the IEG4 Board. These reviews take into account both local and global events to ensure that risks are appropriately assessed, monitored and managed.

g) Use of live data in testing

The Local Authority (LA) is responsible for the provision and management of test data, as this is typically sourced from the back-office systems integrated with the IEG4 platform. IEG4 can advise and support the LA in implementing best practices to ensure compliance with applicable data protection, security, and governance requirements.

h) Incident Management.

IEG4 has a Standard Operating Procedure (SOP) for Incident Management, recently updated to align with ITIL4 more closely. We do operate a unified practice covering IT, security and clinical safety incident management. The SOP outlines how we would react to an incident including what happens were there to be a data breach.

Security Due Diligence and Assessment

IEG4 applies Baseline Personnel Security Standard (BPSS) pre-employment screening to personnel who require access to systems or information containing DWP, HMRC or Home Office-derived data. Screening is completed prior to the relevant access being granted and includes verification of identity, nationality and right-to-work/immigration status, employment history covering the previous three years, and a criminal record check covering unspent convictions. Access to systems and data is controlled in accordance with IEG4's role-based access control and least-privilege principles and is only provided following completion of the required pre-employment checks and authorisation. All personnel are required to complete information security and data protection training as part of their induction and undertake refresher training thereafter. This includes their responsibilities for the secure handling of information, appropriate system use, data protection, confidentiality and the reporting of security incidents. Additional security awareness activities are undertaken throughout the year as part of IEG4's ISO/IEC 27001-certified Information Security Management System.

We trust this document provides the reassurances you require, but please reach out to us if more information is required. The contact on this matter is Alan Powell, our Chief Operating Officer (Alan.Powell@ieg4.com).