G-Cloud - Lot 2b (SaaS)

ISARR Higher Education Institutes - Security & Resilience Platform

Service Definition 2026

ISARR
85 Great Portland Street, First Floor,
London,
W1W 7LT

+44 203 475 0753
g-cloud@isarr.com
www.isarr.com

Higher Education Institutes - Security & Resilience Platform

ISARR work closely with the HEI sector and have developed a custom version of the **Security & Resilience Platform** for the sector, based on deployments with over a dozen UK Universities.

HEI Sector Challenges

The HEI sector has had to adapt quickly to digitisation of key functions over the last several years. Based on our work and engagement with the sector, we have identified a set of common challenges for which we have developed a software and service specifically to address. In order to save you time, and quickly see if the ISARR module meets your operational needs, please consider the following questions based on your current incident management recording, reporting and communication;

Does your current Security & Resilience application or process:

1. Provide high quality, coherent and consistent incident reports at all levels from business as usual to major incidents.
2. Facilitate real time and discrete sharing of information and reports with all key stakeholders across the enterprise to provide immediate situational awareness at all response levels.
3. Enable optional use and custom modules across the University (i.e. Student Services, Health & Safety, Maintenance and on-call Silver & Gold Incident Management Teams).
4. Produce reports that meet first evidence standard in a UK Court, HSE Investigation or Coroner's Court.
5. Have an ability to upload CCTV or video.
6. Provide a management dashboard for analysis and information for senior management – (to support resource justification and trend analysis).
7. Link contextually to Business Continuity Plans and other SOPs.
8. Provide an automated audit trail of all incident reports that are easy to recover (essential for a number of reasons, not least operational learning through lessons identified).
9. Enable easy, intuitive use and operation in a crisis and to facilitate ease of training and operator adoption.
10. Manage information data retention requirements.
11. Meet all GDPR and Cyber Essential requirements.
12. Have a REST API to Integrate with other University systems.

If the answer to any of these challenges resonates then it is highly likely that the module will be able to support, enhance and add value to your operation and the data capture and management of security, safety and wellbeing incidents across the organisation

Incident Management, Logging & Reporting
The Platform supports a range of information sharing, notification, collaboration and management. The core functions within the module are summarised in the diagram below

Bespoke Configuration
The platform benefits from an off the shelf cost, but will detailed customisation and configuration options

Incident/Event/Report Form Details
The routine operations and bespoke forms are completely customised to the organisations operations, including terminology and process. This not only helps to streamline and automate the existing process, but also ensures ease of training and adoption.

Advanced Location Profiles
Locations can be given unique profiles and specific data fields to support a single page view of the current incidents, risks, safety, continuity and resilience information for that location delivery detailed information and operational context

Groups Structure & Permissions
Flexible group structures facilitate the ability to share and restrict all reporting, in addition to granular set of permissions for each group

Administration & Management Support
System Administration can be conducted by nominated individuals so that the organisation is able to carry out a range of management functions.

Uniquely the ISARR support team are also available to reformat report fields, add or edit reporting categories, structure new groups etc. This does not require any additional change requests or costs – ISARR understand that the operating environment will change over time, and our services are built to support this without incurring any additional costs for each configuration

Optional Addons

Single Sign On
SSO can be setup during the initial configuration phase so that users can seamlessly login to the system, by using their existing work credentials.

Integrations and REST API
The platform has an open API which can connect to other systems if required

Data import
Import of existing records is also possible

Example Clients
ISARR has been working with AUCSO, HEBCON and the HEI sector for several years and are proud to count the following Universities as some of our clients

Real World Case Studies

The following examples are based on real events but sanitised for confidential reasons. They demonstrate that accurate information can be shared with alacrity to all appropriate stakeholders to ensure timely action, particularly in issues that may be time sensitive.

Response to potential sexual assault:

The University's First Responders (Security) are called/alerted to a potential sexual assault. Following Standard Operating Procedures (SOPs) the victim is comforted in a safe environment whilst preserving all evidence and the police called. The ISARR incident report can be shared with the police as first evidence, and forwarded immediately, automatically and discreetly to student services for follow-up action as required. The report originator (Security) has no access to any information added by those further in the chain of custody.

Response to potential failure of Health & Safety:

First responders are called to a first-aid incident involving a member of staff. First aid is successfully administered, and an ambulance called. The incident also involved a potential failure of Health & Safety. The ISARR Incident Report is immediately and automatically shared with HR so they are aware of the staff incident, and the Health & Safety Team who can then investigate the incident. The ISARR report can be used as first evidence in an HSE investigation or a litigation claim.

Response to incident of antisocial behaviour and damage to property:

Security are called to an incident of antisocial behaviour by a group of students involving damage to University property. Security disperses and resolves the immediate issue. An ISARR Incident Report is automatically and immediately sent to Academic Services for potential disciplinary action, and to Estates for damage investigation, repair and costing.

Response to major incident in progress:

3am on a Saturday morning, Security responds to a fire alarm and attends the scene to initiate a first response and meet Emergency services. On arrival, it is clear a major incident is in progress. The initial ISARR report and subsequent update are shared immediately and automatically with the on-call Silver and Gold Incident Management Team (regardless of location), ensuring they have appropriate situational awareness in formulating their response and recovery action. Before arriving on site, the Silver Team can continue to communicate with each other which is included in the report audit trail.

Government Classification Level

The ISARR software platform can support the management of information assets at "OFFICIAL" level, with the additional option of "OFFICIAL Sensitive" through agreed local handling arrangements on a project by project basis.

Deployment & Service Model Options
The ISARR software platform is typically deployed in our own UK, private cloud environment that meets and complies with Government assurance and impact level standards. For UK clients this ensures a UK based Data Centre to support GDPR requirements.

Cloud Software as a Service (SaaS)
The ISARR software platform is a web application delivered as a service and accessible from various desktop and mobile clients via a modern web browser and internet connection. All of the underlying cloud infrastructure including network, servers, operating systems, storage, and availability is fully managed as part of the service. The platform is installed as a single application and is not a shared application / database.

Data & Maintenance (see ANNEX A)

Data Centres
The ISARR software platform uses a primary and geographically separate secondary DC in the UK for data sovereignty. The physical security baseline of the data centres include ISO 27001:2013, PCI-DSS v3.2, PSN CoCo and the requirements of data marked OFFICIAL. The data centres individually exceed normal commercial good practise with controls such as IL4 alignment, Class 3 strong-room construction, ANPR vehicle entry controls or the use of vibration sensors on exterior walls.

Network
A geographically resilient, low-latency WAN between both data centres and support locations, with diverse transit locations and a large bandwidth over-provision and DDoS mitigation controls to ensure availability. PSN and HSCN connections are available with simple to use cross-site networking solutions for geographically redundant services. WAF 7G Firewall managed through AWS redundant Load Balancers (UK & EEA) Traffic Routing, AWS Route53 redundant DNS and AWS Shield DDoS mitigation

Compute Resources
Standard VPS is 4GB RAM, 4vCPU Processor and 80GB SSD. This will be configured with a webserver, DB and Load balancer cluster configuration for high availability.

Storage Options
Non-persistent VPS Storage - VPS servers provide non-persistent storage (which means that the data would be removed when the compute resource is terminated)

Persistent Object Storage - Persistent Object Storage provides additional cloud storage, backups and archiving for disaster recovery, by storing a second copy of important business files outside of your business infrastructure within a resilient environment.

Data Durability and Reliability
Copies of data held In logically and physically separate infrastructure. All data is triplicated, ensuring 99.999999% object durability.

Backup/restore and disaster recovery
Backups can be taken as snapshots. By default these are daily with 7 day rotations and 1 monthly backup. In line with High Availability requirements, data can be replicated in real time between database instances. All backups are Encrypted at Rest.

Patching & Updates
ISARR runs a patching framework that prioritises any vulnerability severity and patches these within 24 hours for extreme, 48 hours for high and within 5 days for medium. Details are maintained in our internal register as part of the ISAME Gold accreditation and audit process.

Utilisation monitoring/reporting
Real time resource monitoring is maintained with email Alerts for specific trigger thresholds.

Security
ISARR has a comprehensive physical and data security policy and standards inline with NCSC 14 Cloud Security Principles. Details and copies of the ISARR ISP Assurance framework can be supplied on request. Baseline and Enhanced cybersecurity capabilities include;

Baseline	Enhanced **(Optional)**
- Firewall Groups - Vulnerability Management Programme - Web-Application Firewall OWASP Top 10 - DDoS Mitigation	- 24/7 Protective Monitoring and Virtual Security Operations Centre (SOC) Delivered by a UK-based analyst team, designed for both public and private sector organisations.

Data Privacy & Retention
ISARR are fully compliant with General Data Protection Regulations, with Controller/Processor relationships established under the Terms and Conditions of the contract.
The ISARR software platform also has a custom Data Retention function that allows specific categories to be assigned a retention period that are then automatically flagged for review. This saves considerable manual administration and monitoring of data retention compliance and ensures that this is aligned with the project's policy and requirements.

Service & Support

ISARR provides two levels of Service Level Agreement (SLA) (detailed in the Terms and Conditions document);

- Standard: - Monday to Friday 0900 - 1730 GMT
- Priority: - 24/7 on call with escalation to Cloud Engineer

Setup & Configuration
A comprehensive setup programme captures all of the configuration details for the project, including any existing reporting formats that the client already has, as well as specific terminology and structures. This ensures that the incident management module is aligned with current procedures and streamlines adoption

Onboarding & Training
A custom training package is created in PPT, PDF and Video and is accessible for end users in the system help section. In addition, “train the trainer” packages can be provided.

Service roadmaps
A roadmap will be agreed as part of the project, that will capture ongoing updates and enhancements, as well as any defect resolutions and other key schedules

Termination & Off Boarding
All data is exported and returned to the client, in CSV/Excel format, with additional archives for files and other assets. All remaining data is destroyed in compliance with best practice data security standards with official confirmation provided after destruction

Pricing
ISARR has developed a discounted offering for the Education sector, detailed in the pricing document.

The Pricing model consists of three components;

1. Baseline annual licence fee based size and complexity
2. Additional price per module (with discounts for multi module use)
3. One time setup, configuration and training
4. Message fees (for high volumes of SMS messages)
5. Optional one off integration – for example SSO or Criticalarc SafeZone

Ordering Process
The project is defined and detailed in the signed “Order Form” as part of the T&C’s

Terms of Service
Licence terms are agreed in the order form and follow the current G Cloud terms. The annual licence fee is invoiced (annual) upfront and any overage usage invoiced monthly in arrears

Reference Clients

Client reference can be supplied on request

Further Information

Please email for any specific technical questions: g-cloud@isarr.com

ANNEX A