Cloud Security Principles – Vuelio Platform

The NCSC have developed a set of cloud security principles.
These provide guidance on how to configure, deploy and use cloud services securely
https://www.ncsc.gov.uk/collection/cloud-security
Vuelio take account of these principles in the design, deployment, and operations of their platform.

#	Principle	Description	Evidence of Assurance
1	Data in Transit Protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	Client data is always encrypted when traversing public networks. We use HTTPS with appropriate versions of TLS for this. For internal communication within our cloud hosting environment we have a mixture – some use encrypted transport, others do not. In the cases where encrypted transport is not in use, we have services installed on private subnets with effective firewalls and access controls. In all cases we use TLS 1.2 for encryption of data in transit.
2	Asset Protection and Resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.	Data stored in the Vuelio platform is held in databases, search indexes, and file systems. All data is encrypted at rest using AES-256. All data is regularly backed up, and backups are written to geographically redundant encrypted storage. Client data is stored and processed in cloud IaaS and PaaS solutions – physical security is provided by our cloud platform providers.
3	Separation Between Consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another. If this principle is not implemented, service providers can not prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	Some components of the Vuelio platform follow a single-tenancy implementation pattern. For these components, we have separate data bases, and separate web applications, but on shared virtual servers. Some components of the Vuelio platform follow a multi-tenancy implementation pattern, in which all tenants use the same hardware and software. In this scenario we use data modelling and application design patterns to achieve logical isolation and protection of client data. Code review and Software Quality Assurance processes ensure that design standards are adhered

			to, and effective isolation of client data has been achieved. In all cases, penetration testing is used to ensure effective separation of client data is been achieved.
4	Governance Framework	The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it. If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	Access Intelligence has certification for ISO/IEC 27001:2013.
5	Operational Security	The service provider should have processes and procedures in place to ensure the operational security of the service. If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	Access Intelligence has defined policies and processes to ensure Operational Security: Information Classification – sensitive data is classified and catalogued so that we always know where the data that needs protection resides. Threat Analysis – for each category of data that is stored and processes in the Vuelio platform, the treats are regularly reviewed to ensure effective controls in place to mitigate. Design Standards, Code Review, Quality Assurance and Change Control are all part of standard process for software development and deployment. Access control to ensure the principle of least privilege is upheld. Regular Penetration testing of Vuelio platform to ensure effective controls have been correctly implemented to ensure protection of platform and data. Logging and Audit of platform activities. Automation is used for many procedures for software development and infrastructure management to reduce errors and ensure consistency and repeatability.

			Redundancy and Disaster Recovery has been considered as part of application and infrastructure design.
6	Personnel Security	Service provider staff should be subject to personnel security screening and security education for their role. If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	Personnel security screening is in place for certain defined staff roles where required. All staff receive information security awareness training, and regular refreshers.
7	Secure Development	Services should be designed and developed to identify and mitigate threats to their security. If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	Design Standards, Code Review, Quality Assurance and Change Control are all part of standard process for software development and deployment. Design standards include awareness of the 'OWASP Top Ten' to ensure protection against the most common web threats.
8	Supply Chain Security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	Access Intelligence's technology suppliers are audited to ensure implementation of appropriate controls related to data security. Register of sub-processors: https://www.vuelio.com/uk/vuelio-sub-processors/ We host all services with Microsoft Azure Cloud – they have multiple accreditations associated with data security Ref: https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/
9	Secure Consumer Management	Consumers should be provided with the tools required to help them securely manage their service. If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	The Vuelio platform is provided as a SaaS platform – as such very limited client management is possible or necessary. Within the platform features have been implemented to enable clients to manage the lifecycle of various data types.
10	Identity and Authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals. If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur.	All access to Vuelio platform is subject to authentication and authorisation controls. The platform implements sensible defaults for various elements of access control, these can be customised to client requirement if increased protection is necessary.

			Customisable elements related to authentication: Password complexity Password expiry time Password retry count before lockout Use of Captcha on login after count of login attempts A project is currently in progress to add multi-factor authentication, and federated authentication – this is currently available for some Vuelio Platform modules.
11	External Interface Protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them. If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	Vuelio public services are catalogued. The services are protected by firewalls, and data encryption for transport. Annual 3rd party penetration testing ensures the effectiveness of our controls.
12	Secure Service Administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	Administrative access is only provided to appropriately trained and trusted individuals. Access control methods are implemented to ensure protection. Network routing to servers and databases for administration is constrained to trusted corporate networks, or remote users via VPN.
13	Audit Information Provision to Consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it. If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	The Vuelio platform tracks key events within the platform such as log-in and creating or editing records. These logs are not readily available to end users within the platform. They are however available on request.
14	Secure Use of the Service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected. If this principle is not implemented, the security of cloud services and the data held within	The Vuelio platform is available to consumers as a web application. Consumer organisations are responsible for ensuring effective security controls exist on end-user computers and networks to reduce risk. These might include: Firewalls, authentication controls, anti-malware, web filtering, patching etc.

		them can be undermined by poor use of the service by consumers.	