Data Security Policy

This documents AMAG's Data Security policies, processes, tools, and guidelines implemented to ensure the security of any data AMAG receives, transfers, processes, and stores.

1.0 Purpose

AMAG must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user and employee awareness and avoid accidental loss scenarios. This document outlines the requirements for data breach prevention.

AMAG's intentions for publishing a Data Security Policy are to focus attention on data security. AMAG is committed to protecting AMAG's employees, partners, clients, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Scope

This data security policy applies to all customer data, personal data, or other company data defined as sensitive by AMAG. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.

3.0 Policy

3.1 Principles

- The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

3.2 General

- Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

- The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
- Each user shall read this data security policy and the logon and logoff guidelines, and sign a statement that they understand the conditions of access.
- Records of user access may be used to provide evidence for security incident investigations.
- Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

3.3 Access Control Authorization

- Access to company IT resources and services will be given through the provision of a unique user account and a sufficiently complex password. Accounts are provided by the IT department based on records in the HR department.
- Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Network Access

- All employees and contractors shall be given network access in accordance with business access control procedures and the “least-privilege” or “least-permission” principle.
- Segregation of networks shall be implemented as recommended by the AMAG's network security team. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.
- Network routing controls shall be implemented to support the access control policy.

3.5 User Responsibilities

- All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
- All users must keep their workplace clear of any sensitive or confidential information when they leave.
- All users must keep their passwords confidential and not share them.

3.6 Application and Information Access

- All company staff and contractors shall be granted access to the data and applications required for their job roles.
- All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.
- Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.7 Access to Confidential, Restricted information

- Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

- The responsibility to implement access restrictions lies with the IT Security department.

3.8 Access Control Methods

- Web authentication and authorization
- Database authentication and authorization
- Multi-factor authentication
- Appropriate permissions to files and folders
- Role-based access model
- Server access rights
- Firewall permissions
- Network zone and VLAN ACLs, Virtual Private Networks
- Encryption at rest and in flight
- Network segregation
- Auditing of attempts to log on to any resources on AMAG's networks and/or cloud and infrastructure service accounts

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

4.0 Reporting

- Daily incident reports shall be produced and handled within the information security department or the incident response team.

- Weekly reports detailing all incidents shall be produced by the information security team and sent to the IT manager or director.

- High-priority incidents discovered by the information security team shall be immediately escalated; the IT manager should be contacted as soon as possible.

- The IT Security department shall also produce a monthly report showing the number of IT security incidents and the percentage that were resolved.

5.0 Responsibilities

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.

- **Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.

- **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.

- **The information security team** shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.

6.0 Enforcement

Any AMAG personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their access and network connection terminated.

7.0 Definitions

2-factor Authentication (2FA) - A system that uses 2 forms of authentication to verify user identity. Typically this is a username/password combination and an authentication system tied to a mobile device. See also: Multi-factor authentication.

Multi-factor Authentication (MFA) – a system that uses multiple forms of authentication to verify a user's identity.

Access control list (ACL) — A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.

Database — An organized collection of data, generally stored and accessed electronically from a computer system.

Encryption—The process of encoding a message or other information so that only authorized parties can access it.

Firewall — A technology used for isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.

Least-permissions principle - A subject or user should only be granted privileges sufficient to complete its task.

Least-privilege principle - see "least-permissions" principle.

Network segregation — The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for

technical support and another zone for research, each of which has different technical needs.

Role-based access control (RBAC) — A policy-neutral access-control mechanism defined around roles and privileges.

Server — A computer program or a device that provides functionality for other programs or devices, called clients.

Virtual private network (VPN) — A secure private network connection across a public network.

Virtual private cloud (VPC) — An isolated group of resources typically based in a cloud service.

VLAN (virtual LAN) — A logical grouping of devices in the same broadcast domain.

6.0 Revision History

Version	Date of Revision	Author	Changes
1.0	July 22nd 2020	Jared Keller	Initial version