elucidate

Data Management and Security Policy

Introduction

At Elucidate Group, we are committed to providing top-tier software implementation consulting services to our business partners and clients. Central to our commitment is the effective management and protection of data. This Data Management and Security Policy outlines the principles and practices we employ to safeguard the confidentiality, integrity, and availability of data entrusted to us.

1. Data Classification

We classify data into three categories:

1. Confidential Data: Data that requires the highest level of protection, including sensitive client information, proprietary business data, and financial information.

2. Internal Data: Data intended for internal use, such as project-related documents and non-sensitive client information.

3. Public Data: Data that can be shared with the public, such as marketing materials and non-sensitive, non-proprietary information.

2. Data Handling:

- All employees are responsible for ensuring that the data they handle is appropriately classified and protected.

- Confidential data must be encrypted and stored in secure locations, and access is granted on a need-to-know basis.

- Data can be transferred only through secure channels, and its transmission should be logged and monitored.

- Data retention and disposal policies are established to ensure data is not retained longer than necessary.

3. Access Control:

- User access is granted based on their roles and responsibilities, and it is regularly reviewed and updated.

- Multi-factor authentication is used for critical systems and sensitive data access.

- Access logs are maintained, and suspicious activities are investigated promptly.

4. Data Backup and Recovery:

- Regular data backups are conducted to ensure data recoverability in case of data loss or system failure.

- Data restoration procedures are regularly tested to ensure rapid recovery.

5. Data Privacy:

- Compliance with relevant data privacy laws, including GDPR is a top priority.

- Client data is only used for the purpose for which it was collected, and consent is obtained as necessary.

- Data breach response plans are in place to handle potential data breaches efficiently and effectively.

6. Security Awareness:

- All employees receive regular data security training.

- Reporting mechanisms for security incidents and data breaches are in place to promote a culture of vigilance and accountability.

7. Vendor Management:

- Third-party vendors and service providers that handle data on our behalf are carefully vetted for their security practices.

- Vendor contracts include data protection clauses and stipulations for regular security audits.

8. Security Audits and Testing:

- Regular security audits and vulnerability assessments are conducted to identify and address security weaknesses.

- Penetration testing to be carried out on request.

9. Policy Review and Updates:

- This policy will be reviewed annually and updated as needed to reflect changes in technology, regulations, and best practices.

At Elucidate Group, we are dedicated to maintaining the highest standards of data management and security. We take every possible measure to protect the data entrusted to us by our business partners and clients. By adhering to this policy, we ensure the confidentiality, integrity, and availability of data and contribute to the trust and satisfaction of our stakeholders.

If you have any questions or concerns regarding our Data Management and Security Policy, please contact Nick Dalton..

nick@elucidategroup.com.au
0417748639

Elucidate Group