Esri UK and Esri Ireland Information Security Policy for Suppliers

Introduction

All supplier employees and third-party contractors have an obligation to protect Esri UK and Esri Ireland information, assets, systems and infrastructure. At all times, they will act in a responsible, professional and security conscious manner outlined in this policy.

Failure to comply with this policy could unduly expose Esri UK or Esri Ireland to increased risks from security incidents, including the compromise of the confidentiality, integrity and availability of information systems and/or data.

Suppliers should report any security concerns in relation to Esri UK IT systems, processes or policies to the CIO or CISO by emailing cybersecurity@esriuk.com

General Requirements

- The supplier will complete a security questionnaire, provided by Esri UK, which will be reviewed bi-annually
- The supplier shall implement and maintain appropriate best practice technical and organisational measures in order to meet the requirements of this policy. The supplier should be accredited to ISO 27001:2013 or be using it as a framework for guiding their approach to managing information security.
- If UK based, the supplier should be Cyber Essentials certified and, if not already, be working towards Cyber Essentials Plus.
- All staff working on Esri UK systems should have completed an agreed security background check
- The supplier must comply with all applicable data protection laws
- The supplier shall maintain a Business Continuity Plan for all relevant services
- The supplier shall provide a security representative as the single point of contact for Esri UK on all security issues, who shall be responsible for overseeing compliance with this policy
- The supplier shall provide regular training to their staff (at least bi-annually) on information security best practices and principles
- The supplier shall maintain appropriate physical security controls to prevent unauthorized physical access to assets used to access Esri UK systems
- The supplier will implement appropriate processes to respond to and manage information security incidents, including unauthorized or improper access to or use, handling, or disclosure of Esri UK information assets or IT systems
- Any Statement of Work (SoW) may require additional privacy and security controls, which shall be mutually decided by the parties and defined in the SoW
- Esri UK may, at its expense, perform an audit of the supplier's relevant operations as they pertain to the Services provided

Access Control

- Do not share any UserID's or passwords used to access Esri UK IT systems
- Do not use any utility programs which override the IT access controls put in place by the Esri UK IS Team
- Do not try to circumvent any Multi-Factor-Authentication used by Esri UK to access IT systems
- Do not use personal devices to access Esri UK IT systems

Computer Use Policy

- Ensure all supplier hardware used to access Esri UK IT systems have best practice security controls implemented
- Do not use any Esri UK IT systems in a way that could cause distress or legal issues to Esri UK or Esri Ireland
- Do not use any Esri UK IT systems in a way that might cast Esri UK or Esri Ireland in a bad light, including accessing sexually explicit, discriminatory, racist, violent, or other similar content

Password Policy

- All user credentials provided by Esri UK should be stored in an appropriate corporate password manager/vault solution used by the supplier
- All user credentials provided by Esri UK should be purged from all devices and any password manager/vault at the end of the contract or earlier when specified by Esri UK
- Where provided, Multi Factor Authentication (MFA) should be set up and used for the system being accessed
- Do not share user credentials to access Esri UK systems with other users
- All passwords shall have best practice controls on length, complexity, expiration, reuse, and lockouts