ESD Information Security Brief

If applicable, the Standards, Policies and requirements outlined in this document apply.

All engagements with ESD that have a data or IT component are subject at a minimum to the following security standards and guidelines as they relate to the safeguarding of ESD information and resources. Additional deliveries that are applicable to the project should be identified from ESD's IT Deliverables Standard within 30 days of contract signing, documented as milestones in the project plan, and delivered in alignment with ESD business requirements. The IT Deliverables Standard will be provided to prospective vendors upon request. Vendor may demonstrate and satisfy compliance with the standards outlined below utilizing comparable Security Standards if approved by ESD's CISO.

- Security Compliance
  - Partners, contractors, vendors, suppliers and all other 3rd parties working with ESD or ESD's contracted vendors must comply with ISO Standards 27001, 27005 and 27035 as they relate to the protection of ESD's network, data and information systems. For more information about these and other ISO standards visit https://www.iso.org
  - Use of AI shall comply with all applicable State and Federal Laws and if applicable ESD policies
  - Must have monitoring process in place and documented for 3rd party compliance
  - If applicable, must provide Identity Access Management, including authentication and transaction auditing
  - Must provide documentation certifying that all 3rd party vendors in the supply chain are complying with ISO standards 27001, 27005 and 27035 as related to their role in the project
  - Must comply with GDPR standards for data collection and protection. For more information about GDPR please visit https://gdpr.eu/
    - GDPR is applicable when developing or using a system that is collecting or storing information from entities or citizens that fall within the scope of GDPR governance.
  - Must adhere to NYS and Federal Cyber Security and Information Security Polices and Laws
  - Must document all 3rd party access to ESD data or information systems
  - Must manage Information Communications to maintain the security of ESD data