ESD IT Project Deliverable Criteria

In addition to a list of mandatory business requirements for any ESD contract or project with an IT component, the following deliverables should be evaluated for inclusion in the Statement of Work (SOW) and if necessary, be further clarified based on specific project requirements. The Security Management Plan and Project Approach deliverables are due withing 30 days of contract signing. All other deliverables that are applicable to the project should be identified within 30 days of contract signing, documented as milestones in the project plan, and delivered in alignment with ESD business requirements.

- Mandatory Deliverable-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
  - Must have monitoring process in place and documented for 3rd party compliance
  - 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 document all 3rd party access to ESD data or information systems
  - Must manage Information Communications to maintain the security of ESD data
  - When accessing ESD systems, vendors, third-party service providers and subcontractors must comply with all city, state and federal regulations, and ESD policies concerning computers and related technologies.
- Mandatory Deliverable – Security Management Plan
  - Must be received within 30 days of contract signing
  - Data Security model, including classification, controls and encryption
  - Data Retention
  - Transaction Security including definition of user roles
  - Physical Security, including disaster recovery, continuity and backups
  - Identity Access Management, including authentication and transaction auditing
  - Secure access to platform must be provided, managed and documented
  - Passwords must be at least 14 characters in length, comprising of at least 1 upper case, 1 lower case, 1 number and a special character. Do **not** use the "&" symbol. Passwords are required to be changed on an annual basis.
  - Systems used by ESD staff must have Multifactor Authentication
  - Patch Management approach
  - Security Logging
  - Vulnerability Scanning, monitoring and remediation
    - Vulnerability Management and Remediation must meet the service level requirements based on prioritization and severity classification of risk outlined in the ESD Security Vulnerability Management and Remediation Service Level Agreement (SLA)
    - Penetration testing should be done on an annual basis with summary reporting and remediation plan of critical issues provided to ESD.
  - Adherence to ESD, NYS and Federal Cyber Security and Information Security Polices and Laws
- Mandatory Deliverable – Artificial Intelligence (AI)
    - AI use shall comply with all applicable State and Federal Laws and ESD policies.
    - AI use shall be purposeful and related to improving ESD's operational and business functions.
    - Use of ESD AI tools for personal endeavors is not permitted.

    - AI use shall have Human Oversight. Decisions that impact ESD, NYS or the public should not be made without oversight by appropriate ESD decision makers. Automated final decision systems are not permitted.
    - Anything that is created by use of AI is intellectual property owned by ESD.
- Deliverable – Project Approach
    - Must be received within 30 day of contract signing
    - Deliverables Approach
    - Criteria for Deliverable Acceptance
    - Technical Approach
    - Issue Management
    - Risk Management
    - Secure System Development Life Cycle
    - Quality Assurance Approach
    - Communications Approach (Project Kickoff, Status Reporting, etc.)
    - Project Schedule
    - Resources must be based in North America
- Deliverable – Change Management
    - All requests for a new scope of work, or a change to an existing scope of work, that has any form of IT related component or service no matter how small, require the prior involvement and approval of IT. This pertains to all ESD stakeholders, 3rd party vendors and any sub vendors being used.
- Deliverable – Business Requirements Validation
    - Refinement of mandatory requirements
- Deliverable – Infrastructure Build & Configuration
    - Hosting Model (on / off premise)
    - Servers
    - Software
    - Hardware
    - Security
- Deliverable – Technical Environments
    - Development / Test
    - Staging
    - Production
- Deliverable – Interface Requirements
    - Does the system need to interface with other ESD or 3rd party Systems?
    - Interface Design
    - Data Migration
- Deliverable – Testing
    - Define testing criteria and approach
- Deliverable – Training
    - Training Plan
    - Training Materials
- Deliverable – Service Level Agreement (SLA)
    - Uptime 99.99%
    - Critical Vulnerabilities: SLA: 15 days
    - High Vulnerabilities: SLA: 30 days
    - Medium Vulnerabilities: SLA: 60 days
    - Low Vulnerabilities: SLA: 90 days
    - Monthly reporting of SLA activities
    - Penalties for not meeting SLA criteria
- Deliverable – Support
    - Define support levels and responsibility

- Deliverable – Implemented System
  - Fully functional production system
- Deliverable – End of Contract Transition
  - Documentation outlining procedures and timelines for returning all ESD owned systems, software, equipment, licenses, data and intellectual property back to ESD
  - Agreed upon data format for returned information
  - Policy for final purging of ESD data from 3rd party systems, backups and disaster recovery sites
- Deliverable Web Project -Google Analytics
  - ESD Google Analytics, Tag Manager and Webmasters Tools account should be used for the analytics reporting aspect of any web project.
- Deliverable Web Project -Images, Artwork, Animation, Maps, Look and Feel, User Experience (UX)
  - All images, original layered image files, look and feel and outward presence (User Experience UX) are the property of ESD. ESD may use, at its discretion the site, graphics, layout and elements for collateral items, including but not exclusive to print, digital and all manner of Broadcast Media.
- Deliverable Web Project-Availability
  - Any network-based information systems, applications developed, or programming delivered to ESD, will comply with Section 508 of the Rehabilitation Act of 1973. This Act states that State Entity Information Communication Technology shall be accessible to persons with disabilities as determined by accessibility compliance testing. For more information visit https://www.fcc.gov/general/section-508-rehabilitation-act.
  - All websites and web applications must conform to Level AA standards of the Web Content Accessibility Guidelines (WCAG). For more information visit http://www.w3.org/WAI/WCAG21/quickref/