RFP Information Security Requirements

Office of Information Security
Division of Instructional and Information Technology
NYC Department of Education

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

Table of Contents

1. About This Document

1.1 Owner & Contact

The owner of this document is:

Desmond White, CISO, DIIT
dwhite2@schools.nyc.gov

1.2 Classification Notice

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

2. Purpose

The purpose of this document is to define the NYC Department of Educaiton's ("DOE") information security requirements for vendors who wish to provide IT products, services or support to the DOE. All vendors awarded a contract to provide such services to the DOE must comply with the policies set forth in this document. At its discretion, the DOE may require vendors to implement, comply with, and/or provide proof of one or more of the requirements laid out in this document.

3. Terminology

A. Application – means software that performs a user-facing function, such as a web application

B. Confidential Information or Data –means any personally identifiable information related to DOE students, student families/guardians, DOE employees, agents and/or volunteers obtained by or furnished to the Vendor; all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-read-able form; and all information marked "confidential" by the DOE. Confidential Information includes, but is not limited to, names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspond¬ence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, and any other information that constitutes "personally identifiable information" as defined in or pursuant to the Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 C.F.R. Part 99) (collectively, "FERPA"), or "personally identifying information" as defined or used in New York Education Law 3012-c; regardless of whether such information was disclosed prior to, concurrent with or subsequent to this Agreement. Confidential Information does not include any information that is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Vendor in breach of this agreement, (ii) demonstrated to have been known to the Vendor prior to disclosure by or through the DOE, (iii) disclosed with the prior written approval of the DOE, (iv) demonstrated to have been independently developed by the Vendor without reference to the Confidential Information, (v) disclosed to the Vendor by a third party under conditions permitting such disclosure, without breach of this agreement, and/or (vi) disclosed as required by court order, subpoena, other validly issued administrative or judicial notice or order and/or as a matter of applicable law; provided, however, that in the event disclosure is required of the Vendor under the provision of any law or court order, the Vendor will (a) promptly notify the BOE of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the BOE to seek a protective order, and (b) disclose such Confidential Information only to the extent allowed under a protective order, if any, or necessary to comply with the law or court order; Notwithstanding the previous sentence, "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2d, or "personally identifying information" as defined or used in New York Education Law §3012-c remains Confidential Information notwithstanding (A) the applicability of items (i), (ii), (iii) and (vi) in the previous sentence, and (B) items (iv) and (v) of the previous sentence to the extent that such disclosures were made at the direction of or such information was maintained on behalf of the DOE.

C. DOE – means the Board of Education of the City of New York (a.k.a. the NYC Department of Education).

D. DOE Users – means all people with an existing account in the DOE Identity Management System. This includes most teachers, administrative staff, on-site contractors and parents.

E. **FERPA** – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

F. **Handle** –means (in the context of Confidential Information) to create, view, modify, store, transmit or delete

G. **PII** – means personally identifiable information, as defined under FERPA.

H. **System** – means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

I. **Vendor** – means an entity awarded a contract by the DOE to provide a product, service or work for the DOE.

4. Note on Security & Privacy

DOE systems and Applications may contain sensitive data, including records of academic performance, medical, legal, criminal and family details and proprietary and confidential internal records concerning DOE students and employees, in addition to information that is confidential by law.

Failure to protect Confidential Infromation from unauthorized disclosure or abuse can have severe legal, financial and reputation consequences for the DOE, itsstudents, families, employees and the Vendor.

5. Relevant Laws, Regulation, Policies and Standards

A. **Family Education Rights and Privacy Act (FERPA)**

FERPA is the primary federal legislation that governs the privacy of educational records. The Vendor must hold all PII obtained, learned or developed by the Vendor in confidence pursuant to applicable provisions of FERPA. The Vendor understands that the release of PII to persons or agencies not authorized to receive such information is a violation of US federal law. Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to return PII to the DOE, when no longer needed or at the expiration of any contract. Vendor understands that upon request, it must permit DOE access to PII that it holds, in order for DOE to meet other obligations under FERPA or pursuant to law.

B. **New York Education Law § 3012-c(10)**

New York Education Law § 3012-c(10) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Vendor understands that to the extent that information protected under New York State Education Law §3012-c(10) is shared with Vendor, Vendor is responsible for complying with this law. Vendor further understands that New York State Education Law § 2-d imposes additional requirements concerning such Confidential Information.

C. New York State Education Law § 2-d

New York State Education Law §2-d is a state law that imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(10), including a number of requirements and obligations that apply directly to Vendor. Vendor understands that it is required to comply with the requirements of New York Education Law 2-d and any regulations promulgated thereunder. Vendor understands that among other requirements, New York Education Law §2-d requires Vendor to:

- Limit internal access to Confidential Information covered under Education Law §2-d ("Covered Confidential Information") to those with legitimate educational interests;
- Not use Covered Confidential Information for any other purposes than those authorized in its contract;
- Not disclose Covered Confidential Information without parental consent, except to authorized representatives of the Vendor who are carrying out the contract;
- Maintain reasonable technical, administrative and physical safeguards to protect Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for marketing purposes;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified under HIPAA by the US Department of Health and Human Services; and
- Notify the DOE of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse DOE for the full notification cost.

Vendor also agrees to cooperate with the DOE in complying with any regulations implementing New York Education Law § 2-d and any DOE or state policies promulgated pursuant to New York Education Law § 2-d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Vendor's contract with the DOE, (b) its compliance with any future DOE data privacy/security policy, (c) its compliance with and signature of the Parent Bill of Rights required of the DOE, and (d) the inclusion of supplemental information concerning Vendor's contract in the Parent Bill of Rights.

A. DOITT Citywide Information Security Policies & and DOE RFP Information Security Requirements

At all locations where Vendor stores any Confidential Information, the Vendor shall implement information security policies and procedures that, at a minimum, are at least rigorous as the DOITT Citywide Information Security Policies, accessible at: http://www.nyc.gov/html/doitt/html/business/security.shtml, and/or this document (Request for Proposals ("RFP") Information Security Requirements).

B. DOE Chancellor's Regulation A-820

The Vendor must comply with the DOE Chancellor's Regulation A-820, accessible at http://docs.nycenet.edu/docushare/dsweb/Get/Document-44/A-820.pdf, which governs access to and the disclosure of information contained in student records.

C. NYSED Records Retention and Disposition Schedule ED-1

Schedule ED-1 specifies which information must be preserved for long periods of time in order to ensure business continuity, resolve fiscal and administrative questions and provide evidence in the event of litigation.

D. **DIIT SAML Integration Guidelines**

This is a technical document that specifies authentication options for integration with DOE Systems. Vendor must support authentication for DOE users as specified in the such document, set forth below in Section 18.

E. **DOE Secure Coding Standard**

This document defines mandated secure coding practices for all Applications that Handle Confidential Information. Code for Applications that Handle Confidential Information must comply with with such standard. The DOE's Secure Coding Standard is set forth below in Section 19 as an example. Vendors can use this as a reference.

6. Information Security Policies

A. Vendors must have, and upon request by the DOE shall promptly provide the DOE with copies of its, information security policies that cover the following elements:

1. Data classification and privacy
2. Security training and awareness
3. Systems administration, patching and configuration
4. Application development and code review
5. Incident response
6. Workstation management, mobile devices and antivirus
7. Backups, disaster recovery and business continuity
8. Regular audits and testing
9. Requirements for third-party business partners and contractors
10. Compliance with information security or privacy laws, rules, regulations or standards
11. Any other information security policies

B. Policy Requirements: In addition to addressing the elements set forth above:

1. Vendor must indicate in their policies the date of the most recent revision.
2. Vendor must include a certification from its Chief Operating Officer, or individual with an equivelant title with authority to represent the Vendor, with Vendor's proposal/response to the RFP that all of the above elements are addressed in Vendor's security policies, and that such policies are at least as rigorous as the policies set forth in this document and the NYC DoITT Citywide Information Security Policies. If Vendor cannot make such certification for any reason (e.g Vendor's policies do not address an element listed above), Vendor must notify the DOE of the deficiency in its proposal/response to the RFP.
3. Vendor shall maintain compliance with such policies and, unless the Vendor receives the DOE's prior written approval, Vendor shall not make any changes to such policies that would result in in such policies (i) not addressing one or more elements set forth above or (ii) not being as rigorous as the policies set forth in this document or the NYC DoITT Citywide Information Security Policies.

7. Privacy & Confidentiality

A. The Vendor must hold Confidential Information in strict confidence and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.

B. The Vendor shall use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to

breaches by unauthorized access or making unauthorized modifications to such System.

C. The Vendor shall protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.

D. The Vendor shall maintain all copies or reproductions of Confidential Information with the same security it maintains the originals. At the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by DOE, Vendor must destroy such Data, making it unusable and unrecoverable.

E. For all Application screens, front pages of reports, and landing pages of web Applications that contain Confidential Information, Vendor must include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).

F. All web Application screens that contain Confidential Information must be non-cacheable.

G. Confidential Information should not appear in URLs.

H. Vendor's development, test and QA environments shall not use real Confidential Information.

8. Application Development

A. Vendors shall have a comprehensive secure development lifecycle System in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle System itself.

B. Code for Applications that handle Confidential Information must comply with the DOE Secure Coding Standard. Any exceptions to this standard must be approved in writing by the DOE.

C. Vendor must review and test all application code for security weaknesses and backdoors prior to deployment with DOE. All high risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of Vendor must certify in writing to the DOE that a security review has been conducted and that all risks are acceptable before every release. For further information please refer to National Institute of Standards and Technology ("NIST") Special Publication 800-64 Revision 2.

D. Vendors that handle Confidential Information must respond to and resolve security-related bug reports, inquiries and incidents in a timely and professional manner. The Vendor must notify the DOE within 24 hours of when Vendor becomes aware of any such incident that poses a potential risk to DOE data. The Vendor shall send the notification to sppsecurity@schools.nyc.gov.

9. Authentication & Identity Management

A. If an application requires Single Sign-On (SSO) integration with the DOE, the Vendor must support authentication for DOE Users as specified in the DIIT SAML Integration Guidelines
   1. Vendors will not have the ability to make any changes to the DOE Identity Management Systems.
   2. If new DOE Users need to be enrolled or register in order to use a Vendor's System, the plan for registration process and ownership of identity management must be agreed upon in writing by DIIT Office of Information Security.

B. If the Vendor maintains its own identity management system for its users, it must:
   1. Enforce a one user, one account policy in which shared/ group accounts and duplicate accounts are not permitted
   2. Be free of testing, development and non-production accounts.
   3. Maintain accurate legal name, address, phone number information for all users who are permitted to access Confidential Information, and upon request from the DOE, produce lists of users who will have access to Confidential Information.
   4. Enforce a strong password policy of eight characters minimum, with mixed case and at least one number or special character.
   5. Store all passwords in non-reversible one-way cryptographic hash.
   6. Log all successful and failed authentication attempts, including date, time, IP address, and username.
   7. Offer a secure password reset feature, including verification of identity, email or text notification and a one-time-use password link that expires after 24 hours.
   8. Automatically de-provision accounts for terminated employees of Vendor and DOE.
   9. Temporarily lock accounts with repeated failed login attempts and provide support to affected users.
   10. Keep attributes and group structures that support authorization accurate.

10. Confidential Information Authorization

A. Applications that Handle Confidential Information must have explicitly defined authorization controls that prevent users from exceeding their intended privileges.

B. Applications must perform authorization checks before performing any action that creates, views, updates, transmits or deletes Confidential Information. Authorization logic must be highly configurable and alterable without code changes.

C. Authorization checks must verify the user has appropriate role to perform the requested action, and also the correct scope. Scope authorization checks should reference DOE location codes, student-teacher-class linkage, parent-student linkage and other data sources.

D. Whenever possible, authorization checks will use the DOE RBAC framework, DOE identity management system and other DOE Systems of record. Access to these Systems may be either via a web service or replicated database, at the DOE's discretion. The Vendor Application will not be able to make any changes to the contents of these Systems.

E. Any non-DOE accounts that are managed locally by the Vendor must follow the the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. "Super users" (i.e. application administrators) must be avoided unless absolutely necessary due to a legitimate administrative or educational need for such access in order to provide the Services.

11. Incident Response

A. Vendors must have a plan for compliance with all applicable breach notification laws, including New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).

B. The DOE must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Confidential Information or a System that supports it.

C. Response actions to incidents that might affect Confidential Information or Systems must be conducted quickly and with ample resources. Vendor will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.

D. DOE shall have the right to view all incident response evidence, reports, communications and related materials upon request.

E. If requested by the DOE, or if required by law, the Vendor shall notify in writing all persons affected by the incident, at its own cost and expense.

12. Audit & Inspection

A. The Vendor shall allow DOE, upon reasonable notice, to perform security assessments or audits of Systems that Handle or support Confidential Information. Such an assessment shall be conducted by an independent 3rd party agreed upon by the Vendor and the DOE, and at the DOE's own expense, *provided* that the Vendor cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel and information needed to ensure the successful completion of the assessments or audits.

B. The Vendor shall provide DOE, upon DOE's request, with a SSAE 16 or similar report as agreed to by DOE for critical business processes relating to protection of Confidential Information and safeguards implemented in its organization.

C. Vendors must engage an independent third party annually to assess the practical security of Vendor's Systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that Handle Confidential Information. Such annual assessment shall be at Vendor's sole expense.

D. Audit logs must be implemented for all Systems that Handle Confidential Information. All attempted violations of System security must generate an audit log. Audit logs must be secured against unauthorized access or modification.

E. In the event of adverse findings through a DOE or Vendor audit, the Vendor shall cooperate with the DOE in remediating any risks to Confidential Information, including complying with request to temporarily taking the system offline or otherwise limiting access to the system, and any other follow up actions reasonably necessary to secure the Confidential Information.

13. Availability

A. Vendor Systems that Handle Confidential Information shall be available and fully functional 24x7x365 with 99.99% uptime, unless otherwise agreed upon in writing with the DOE. Vendor shall make plans for colocation, backups and any other Systems necessary to ensure continuity.

B. Vendor must notify and obtain agreement from the DOE for any planned interruptions in service, with the exception of emergency security updates. Vendor must notify the DOE immediately of any unintended service interruption.

14. Encryption

A. All Systems that Handle Confidential Information must encrypt the DOE data that include Confidential Information in transit using algorithms and key lengths consistent with the most recent NIST guidelines.

B. For HTTP and other protocols that use SSL/TLS, Vendor shall use the TLS 1.1 or later protocol with 128-bit or larger key size, and shall make previous protocols and smaller keys unavailable.

C. Vendor shall utilize a third party provider that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication between two parties (e.g., Vendor and the DOE or Vendor and any other party).

D. Web Applications that contain Confidential Information must be available only over Transport Layer Security ("TLS"). Attempts to use the Application without encryption shall be rejected. Encrypted and non-encrypted content shall not be mixed.

E. Data at rest that is stored outside of hardened Application or database production Systems must be protected by encryption consistent with NIST recommendations.

F. The Vendor shall keep private keys confidential, implement key lifecycle management and protect all keys in storage or in transit.

G. The Vendor shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.

H. Encryption of the DOE data in production databases is *not* required. Any database encryption system must be approved by the DOE, which approval shall not be unreasonably withheld. The DOE must be provided with a complete set of decryption keys. All DOE data must be recoverable.

I. In the event that Vendor will store DOE data outside of the United States, Vendor shall notify the DOE of the locations outside the U.S. by providing notice either in its proposal to the RFP if known by Vendor prior to award, or if known after award, to appsecurity@schools.nyc.gov; *provided* that the DOE reserves the right to require that the use, storage, or handling of DOE data occur within the contiguous United States or similar regional boundary as defined by the DOE, which, if applicable, shall be specified in the RFP.

15. Data retention

A. Vendors may be required to support retention of Confidential Information as per NYSED Education Data Retention Schedule ED-1.

B. Retention requirements for DOE data may be specified in the RFP. If applicable, the Vendor must acknowledge in its proposal to the RFP that it can meet the requirements and, upon request by the DOE, demonstrate that retention requirements are being implemented.

C. Record retention systems must comply with all security and privacy controls set forth in this document.

16. System Configuration & Maintenance

A. All operating Systems, servers, and network devices that support DOE Systems or Confidential Information must be kept hardened and patched.

B. All Vendor Systems that are used to host, transfer, or otherwise interact with Confidential Information must enforce strict separation from any non-DOE Systems. This can be achieved through physical and/or logical separation. The separation must be auditable and able to be proven at the request of the DOE.

C. Vendors must maintain technical best security practices configuration guidelines for all such Systems and update them at least twice per year.

D. All security-related patches must be installed on Systems within 24 hours of their release. Vendor will maintain a testing lab in order to support this.

17. Subcontractors

A. In addition to the subcontracting provisions in the agreement with the DOE (which require DOE approval of all subcontractors), in the event that a Vendor utilizes subcontractors to support a System that Handles Confidential Information (each a "subcontractor"), such subcontractors shall be subject to, and Vendor must require that each subcontractor comply with, the requirements set forth herein.

18. Appendix (A) – DIIT SAML Integration Guidelines

"SAML" – means Security Assertion Markup Language

SAML allows Single Sign-On between Partner Websites and through this allowing sharing of user identities to provide a better user experience. SAML can thus be used for:

- Web Single Sign-On (SSO)
- Attribute-based Authorization (followed by Web SSO)
- Securing Web Services

SAML Components

Below is a list of some SAML components included for the purpose of this document.

Assertion

An assertion is a package of information that supplies one or more statements made by a SAML authority (the Identity Provider). The assertion may contain authentication information, attributes for authorization and other information as desired.

Identity Provider

The Identity Provider (or IdP) is the user authenticating authority in a SAML environment, responsible for authenticating a user and providing authorization information. **DOE will assume this role.**
Service Provider

The Service Provider (or SP) is the partner or service that requests for and consumes the user authentication and authorization information, enabling users to access their Website or Web Services without re-authenticating themselves. **The content provider will assume this role.**

Protocols

Defines a number of requests/response protocols that allow service providers to:

- Request from SAML authority one or more assertions.
- Request that an IDP authenticate a principal and return the corresponding assertion.
- Request that a name identifier be registered.
- Request that the use of an identifier be terminated.
- Retrieve a protocol message that has been requested by means of an artifact.
- Request a near-simultaneous logout of a collection of related sessions (Single Logout)
- Request a name identifier mapping.

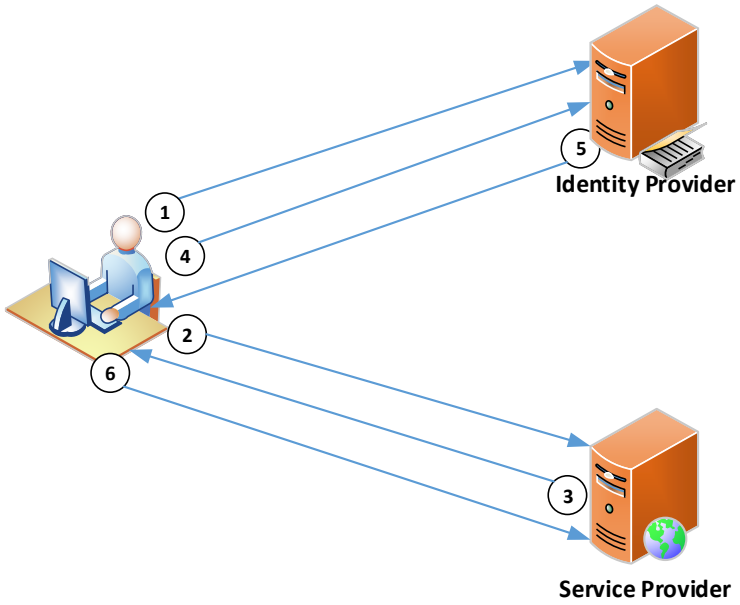
Binding

Defines how the IdP and SP exchange information. The most common bindings are:

- HTTP Redirect (GET) Binding
- HTTP POST Binding
- HTTP Artifact Binding

SAML Flow

The following diagram illustrates the SAML flow from a high-level for the SAML Post Binding with an Identity Provider initiated login.



1. User logins to an SSO Portal (Identity Provider -IdP)
2. User then clicks on a Partner website link (Service Provider- SP)
3. The SP then asks the IdP to authenticate the user sending a signed authentication request.
4. The request is redirected through the user browser to the IdP.
5. The IdP validates the request and sends a signed SAML assertion back (the user would have been challenged for credentials by the IdP if he/she hadn't already logged in).
6. The SAML assertion is redirected to the SP through the user browser. The SP identifies and authorizes the user using information in the assertion and logs in the user

Note: For security purposes it is optimal that all communication occur over a secure channel (HTTPS) and all information be digitally signed by either party.

19. Appendix (B) – DOE Secure Coding Standard

DOE SECURE CODING STANDARD

Office of Information Security
Division of Instructional and Information Technology
NYC Department of Education

CLASSIFICATION: PUBLIC

This document may be distributed without restriction.

Table of Contents

About This Document

Owner & Contact

The owner of this document is:

Kevin Spett
Application Security Engineer
kspett@schools.nyc.gov

Classification Notice

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

Part I: Background

Purpose, Audience & Scope

This document defines requirements for security and privacy in DOE applications. All new development, including enhancements to existing applications, should comply.

This document has been written with web applications in mind, but much of it applies to other types of applications. Note that network infrastructure, operating systems, and server configurations are outside the scope of this standard.

This document is intended for developers at the DOE, whether inside DIIT or another department. It may also be used by third parties that develop or integrate systems which handle DOE data.

Development managers should also familiarize themselves with this standard. Most sections should be understandable without detailed programming knowledge.

References

The following documents have influenced this document or may be useful to its audience:

- **Family Education Rights and Privacy Act (FERPA)**
  FERPA is the primary federal legislation that governs the privacy of educational records.
- **DOITT Citywide Application Development Security Policy**
- **NYSED Records Retention and Disposition Schedule ED-1**
  Schedule ED-1 specifies which information must be preserved for long periods of time in order to ensure business continuity, resolve fiscal and administrative questions and provide evidence in the event of litigation.
- **DIIT Secure Development & Review FAQ**
  This document explains the secure development and review process at the DOE.
- **DOE Data Classification Standard**
  This document defines classifications and handling guidelines for the DOE's data, including public and non-public information.

The Importance Of Security & Privacy

The Department of Education is responsible for protecting the privacy of its 1.1 million students, 135,000+ staff, 1,700+ physical locations and $23+ billion dollars.

DOE systems contain personal data, including medical, legal, criminal and family details, records of academic performance, and proprietary internal records. We must take every possible precaution to protect this information. Failure to do so can have severe physical, legal and financial consequences for the DOE's students, families, employees and the the organization itself.

Technological innovation presents opportunities for improving education and business performance, but also new risks. Please do your part to help protect privacy and security at the DOE.

Security In The Software Lifecycle

The adage "an ounce of prevent is worth a pound of cure" holds true for security in software development. When business owners, development managers and developers think about security and privacy at a project's inception, the

result is the on-time delivery of secure software.

Failure to consider security until the end of the development process may cause a variety of issues that could have been avoided, including delay in release while security issues are fixed.

Project managers should coordinate with the Office of Information Security throughout the development lifecycle, particularly on projects that handle non-public information, perform critical tasks, or are available to a large group of users.

Depending on the risk presented by the application's features and data, the security team may elect to participate at none, all or a few of these stages:

- Origination
- CSD
- Delivery
- Implementation

Please see the *Secure Development and Review FAQ* for more information about security in the development lifecycle.

Deviations from this Secure Coding Standard require written approval from the DOE's Office of Information Security. The Office of Information Security reserves the right to withhold approval of any application that does not comply with the Secure Coding Standard, or contains other unacceptable security or privacy issues.

Questions, Answers and Feedback

If you have questions or comments about the security of an application that handles DOE data or any security or privacy-related question, you can always contact the Office of Information Security.

We also encourage feedback and suggestions about our policies, documents and the process of working with us.

You can contact the following with any feedback:

Application Security Engineer - Kevin Spett (kspett@schools.nyc.gov)
Chief Information Security Officer - Desmond White (dwhite2@schools.nyc.gov).

Part II: Secure Coding

The terms Non-public, Restricted, Sensitive, and Public are defined in the *Data Classification Standard*, which should be read by everyone who develops software for the DOE. For purposes of this document, the term "Confidential Information" defined in Section 3 of the RFP Information Security Requirements means "Restricted" and "Sensitive" information as defined in the Data Classification Standard. The term "Non-public Information" includes Confidential Information, Restricted Information and Sensitive Information.

Privacy Guidelines

- **Privacy features should be clearly defined.** When you begin working on a project, think about what Non-public information it handles, how many users have access to it, and where it will be accessible from.

  Consider the security controls included in the Business Requirements Document (BRD) and Security Requirements Document (SRD). Does it clearly define users, groups, roles and permissions for each operation? Do the permissions make sense? You should be clear on what users have which roles, what tasks a role may perform, and what data a given user may access.

  Think critically about privacy. If the security controls are not clearly defined, or do not seem adequate for the level of risk, please inquire with your manager, the application's business owner, or the Office of Information Security.

- **Keep use of Non-public Information to a minimum.** Do not disclose Non-public data to users that is not explicitly required in the application's specification.
- **Confidential Information should be masked whenever possible.** When working with data that has a Non-public classification, such as social security numbers or passwords, mask the data whenever possible. For example, only display the last four digits of a SSN unless there is a specific need for the entire number.
- **Limit the use of Non-public information on grid screens.** Do not include Non-public Information on grid screens unless it is essential. Keep them on single record detail screens where their use can be logged more carefully, and fewer records can inadvertently be disclosed.
- **Pages with Non-public Information should not be cached.** Any page that contains Non-public information should be served with headers explicitly instructing the browser not to cache it.
- **Non-public Information should not be transmitted in GET query data.** Non-public Information should never be transmitted in GET query strings of HTTP requests. URL and query strings are often logged by browsers, proxy servers, etc…
- **Unauthorized data should not be "hidden" on the client.** Assume that the user can view any data that has been transmitted to the client. HTML comments, "hidden" form fields, ViewState, etc… are insecure and should not be used to protect Non-public Information. Do not send the client any information that the user may not have appropriate permissions to view.
- **Bulk data transfers must have strong security features and be approved by DIIT.** In general, Non-public data should not be downloadable in bulk, or transmitted to third parties. When bulk transfers or downloads are necessary, security controls must be in place. The dataset should be as limited as possible. Transfers or downloads must generate audit logs, have transmission encryption, and the receiving parties must be authenticated and authorized.
- Any transfers of data to third parties outside the DOE, including NYSED, Federal DOE, independent contractors, other NYC agencies, cloud applications and services, etc. must be approved by DIIT prior to implementation.

Authentication

- **Require authentication.** Any application features or data that should not be publicly and anonymously accessible must require username/password authentication.
- **Central Active Directory (CAD).** Most web applications should use CAD as their authentication source. Do not create application-specific authentication sources in SQL databases, text files or other places. Exceptions must be approved by the Office of Information Security prior to development.
- **Federation.** Applications that are hosted by third parties should use Federation via SAML or ADFS for authentication. Federated authentication is useful when a trusted third party maintains its own identity database, or needs to authorize DOE users for its applications. If your project requires Federation, please speak with the Office of Information Security.
- **Use the Authentication Module.** The ASP.Net NYCDOE Authentication module should be used to facilitate common authentication tasks, such as forms-based authentication.
- **Use the Password Reset Tool.** Applications should direct users to the NYCDOE Password Reset tool when users have forgotten their credentials. Applications should not implement their own password reset functionality.
- **Shared accounts are forbidden.** Authentication must identify a unique person. It is never acceptable for people, vendors or other agencies to share accounts or have a "group" account. (Exceptions may be made for data services between applications.)
- **Provisioning.** If your application supports users who do not already have Central Active Directory accounts, such as job applicants, former employees, parents, etc…, please contact the Office of Information Security for guidance.
- **Encrypt credentials in transit.** Credentials such as usernames, passwords and session identifiers should always be encrypted in transit. Passwords should never be sent in the same communication with a username/userID.
- **Requirements for non-standard authentication solutions:**
- **Approval from Office of Information Security.** All applications that do not used Central Active Directory of Federation authentication solutions must be approved by the Office of Information Security.
- **Password storage.** Passwords must never be stored in plaintext. Passwords should be stored as cryptographically salted and hashed values.
- **Password complexity.** Passwords must be complex in character content and length—at least eight characters, mixed case, with at least one number and one punctuation character.
- **Expiration.** Passwords must expire after 90 days.
- **Lockouts.** Accounts should be locked for 30 minutes after five unsuccessful login attempts.
- **Resets.** For user populations that cannot use the DOE Self-Service Password Reset Tool, password resets should use a one-time link. The link should be mailed to the user's pre-registered email address, and remain active for no longer than 24 hours. The reset process should allow the user to enter a new password. Passwords should never be sent in the same communication with a username/userID.
- **Accountability.** Failed login attempts, account lockouts, password reset requests, account enrollment and deletion, and the last successful login must be logged.

Session state:

- **Use platform-supplied state mechanism.** Do not create custom session-state solutions. Use the platform's built-in session management.
- **Timeouts must be reasonable.** Users should be automatically logged out after 15 minutes of inactivity if an application uses Private or Confidential data, and 30 minutes maximum for any application.
- **Session identifiers must only be transmitted in cookies.** Session IDs should be transmitted in cookies in HTTP

headers, and never in URL query string data or POST parameters.

- **Session identifiers must be encrypted in transit.** Session IDs should never be transmitted in plaintext. When cookies are issued, ensure that the "secure" option is set, which instructs the browser to never transmit it without encryption.
- **Require logout feature for forms applications.** If an application uses forms-based authentications, as opposed to NT integrated authentication, users must be given a logout button to end their session.

Authorization

- **Require authorization for application access.** After authentication, the application should verify that the user has an appropriate role to use it. Applications should not be accessible to the entire population of authenticated users. For instance, an application intended to be used exclusively by principals should ensure that teachers cannot access it.
- **Authorize features and operations.** The application should support granular per-operation authorization controls. Permission should be verified before performing Create, Read, Update and/or Delete (CRUD) operations or other important tasks.
- **Authorize scope.** The application should support scope-based authorization controls. Permission should be verified before accessing or manipulating a data record. For instance, if a principal is attempting to access a student's grades, the application should verify that the student is in his or her school.
- **Use DOE Authorization Module.** The DOE Authorization Module, also known as the "RBAC module", provides a variety of features related to users, roles, tasks and locations. It can be used as either a compiled ASP.Net API or web service. It should be used whenever possible.
- **Make authorization configurable.** It should not be necessary to re-code, compile or deploy an application in order to change authorization logic. Authorization Module methods such as IsAuthorizedForTask and GetLocations make this simple.
- **Authorization failures.** Authorization failures should throw an exception, generate a log event, and display a generic error message to the user.
- **Comment authorization needs.** Authorization needs and explanations should be clearly commented in code.

Accountability

- **Require logging for accountability and privacy.** Applications must generate logs for the purposes of accountability and privacy, not just debugging and troubleshooting.
- **Information classification labelling.** Appliations, reports and documents that contain non-public information should always be cleared labeled as per the Data Classification Standard. Reports should always include the name of the user that generated them and the date.

Operations That Require Logging

- **Operations on Non-public Data.** The creation, retrieval, modification or deletion of Non-public data must be carefully tracked.
- **Authentication events.** Failed login attempts, password reset requests, lockouts, user creation / enrollment / deletion and the last successful login should always be logged. (If you are using DOE Federation or Active Directory as an authentication source, you do not need to manually implement this.)
- **Authorization failures.** Any authorization check which fails must be logged.
- **Information to include in log entries.** Log entries should include the date, time, username, IP address, and a

description of the event being logged.

Input Validation

- **Require input validation.** All user- and client-supplied input must be validated before use. This includes data being transmitted in headers, cookies, URL query data, POST form data, hidden form fields, and web service calls. All data is "guilty" until proven innocent.
- **Validation must occur on the server.** Browser-based validation may be useful as an interface feature, but is not effective for security purposes.
- **Reusable modules should include validation.** Any re-usable code component should perform its own validation, even if it may be redundant in some cases. For instance, a modular data-layer helper should always perform validation, because it may be re-used in an application where the web pages do not.
- **"White list" criteria.** Data should always be validated for length and character content using "white list" logic. Specifically permit what is appropriate, and deny anything else by default. Never include non-printable characters, SQL syntax markers, etc. unless there is a good reason.
  For instance, if you're expecting a phone number, validate that the value is no more than 16 characters long and only comprised of digits, hyphens, spaces and parentheses.
- **Transformations.** In some cases where punctuation or unusual characters are necessary, transform them into HTML entities, such as turning a single quote into """.
- **Use Validator tags and Regular Expressions.** Every form field should have a server-side regular expression validator. For input that does not come from a form field, in-line regular expressions tests are the preferred method for input validation.
- **Validation failures.** In general, when input validation fails, the application should stop processing the request and display an error. Only "mend" user data for minor predictable issues, such as removing dashes from a phone number.
- **Comment complex validation needs.** Regular expressions can be difficult to read quickly. Comment any input validation logic that is not immediately intuitive.
- **The use of unmanaged code is prohibited.** Using unmanaged code can introduce buffer overflow vulnerabilities. If a project must use unmanaged code, please speak with the Office of Information Security.

Output Validation

- **Perform output validation.** Many attacks such as cross-site scripting, drive-by downloads and browser exploitation work by feeding malicious data to web applications for display or distribution.
- Be careful when assembling content that uses client-supplied data. Beware of overly long strings, less-than, greater-than, semicolon, parentheses, single quote, double quotes and other HTML and Javascript syntax tokens.
- **Use ASP.Net validation features, white-list regular expressions and encoding.** Normally, ASP.Net will prevent potentially hazardous characters from "breaking out" of form fields, labels and other display controls. However, if you are "manually" generating HTML or Javascript, you need to do this yourself.
- You can use HttpUtility.HTMLEncode to transform non-alphanumeric characters into HTML-safe entities. Use regular expressions to do general sanity checks for character length and content.
- **Require output validation for email.** Carefully validate all data that is used in email messages. Remember that most popular mail clients are either web applications or use embedded web browser controls to display messages.

Database Access

- **String-building is forbidden.** An application should never piece together SQL statements from strings. This creates the risk of SQL injection. Note that string-building can occur inside stored procedures that use EXEC.
  Use stored procedures whenever possible. Stored procedures save the structure of the SQL query on the database. This is the best way to prevent SQL injection. It also offers advantages for organization, performance and granular authorization.
- **If stored procedures are not possible, use prepared statements.** Prepared statements safely separate SQL queries and parameter values. This effectively prevents SQL injection, but does not offer the other advantages of stored procedures.
- **Each application must have its own database account.** Applications may not share database accounts. Each account's permissions should be tightly configured so that it can only access the appropriate databases, tables and procedures.

File Access

- **File paths should be built with extreme caution.** If any client-supplied input is used to construct a file name or path, use strong input validation. Beware of slashes, backslashes and periods. It should never be possible escape the intended directory. Validate using "white list" logic.
- **Store data and report files outside the webroot.** Do not allow users to directly request files for download or view filesystem directories. Have the application act as an intermediary. Data, report and other files for download or reference should always be stored outside of the webroot.
- **Explicitly set permissions on created or uploaded files and directories.** In general, files should be set read-only, and only by the web server's user. Never allow a file to be created with any execute or world-write permissions.
- **Validate uploaded files.** Uploaded files should be checked for file size and type, and scanned for malware if necessary. Consider what would happen if someone uploaded a Word or PDF file with an embedded virus that was widely distributed.

Error Handling

- **Security-related errors should throw exceptions.** Use throw/catch for all security-related exceptions, such authorization failures.
- **Security-related errors should be logged.** See the Accountability section for more details.
- **Technical details should never be displayed to users.** Applications in production should not display verbose error messages that include stack traces, configuration data or other technical information.

Encryption

- **Require TLS.** All applications that require authentication should only be accessible over TLS 1.1 or later with 128-bit or larger key size. The application should reject attempts to use it over non-TLS connections. Cookies must never be set or transmitted without TLS, prior to authentication and encryption.
- **Use platform-supplied encryption tools.** If an application requires encryption, use the ASP.Net encryption libraries. Do not attempt to write your own encryption routines or random-number generators.
- **Seek guidance about complex encryption needs.** If you're considering using database encryption, symmetric encryption for distributed files, or any other potentially complicated encryption system, please speak with the

Office of Information Security.

- **Do not use insecure FTP**. Regular FTP does not use encryption. This means that all passwords and data are transmitted in clear text. Use a web-based file distribution system, FTPS, SFTP or FTP over SSH instead.