Policy Governing Access to SDA PMWeb Systems

Issued By: Information Systems Division

Policy No.: 1208

Effective Date: September 20, 2023

I. Purpose:

The purpose of the Schools Development Authority (the "SDA") Policy Governing Access to SDA PMWeb Systems (the "Policy") is to establish and reinforce effective guidelines, procedures and responsibilities for access to the PMWeb Systems and/or database(s) of the SDA.

II. Summary:

The Policy provides comprehensive directives and goals for authorized SDA employee and non-SDA Personnel access to the SDA PMWeb Systems and/or database(s) ("SDA PMWeb Systems"). The Policy addresses access authorization, requirements, requests, and responsibilities in connection with the SDA PMWeb Systems.

III. Definitions:

As used in the Policy, unless the context clearly requires a different meaning, the following terms shall have the meaning indicated:

Information Systems – SDA-owned or leased computer hardware, software, telecommunications and wireless equipment, or other electronic media, and the information and data contained therein.

non-SDA Personnel – Individuals not employed directly by the SDA that provide professional services to, or on behalf of, the SDA, *and* contractors, temporary workers and/or consultants who are engaged by the SDA.

PMWeb User – An individual who is authorized by the SDA in accordance with the Policy to use SDA PMWeb Systems and who has acknowledged that they have read, understand and agree to comply with the Policy Governing SDA Network Security or the Policy Governing SDA Network Access for non-SDA Personnel, as applicable to that PMWeb User.

SDA Authorized Representative – SDA Director-level employees and above responsible for managing SDA employees and/or non-SDA Personnel.

Data – Information stored electronically, including, but not limited to, files, images and photographs.

Database – A collection of information and data that is organized so that it can be easily accessed, managed, and updated. Examples of databases that are accessible through SDA PMWeb Systems include PMWeb, and Project Scheduler (also denoted as Primavera P6).

Internet – The worldwide system of interconnected computer networks in which a user at any one computer with an Internet connection can connect with another user at any other computer with an Internet connection to obtain and exchange information.

Password – A string of characters or words that must be used by a PMWeb User to authenticate full or partial access to an SDA computer system or its data resources. For purposes of this definition, a "complex password" means a combination of upper case and lower case letters, numbers, and symbols, with the exception of an asterisk (*), ampersand (&) and pound sign (#).

User Account – A unique user log-in account created for a PMWeb User that enables the user to access SDA PMWeb Systems remotely, in accordance with the permissions prescribed for their specific approved role.

Technology Request Form – A form used by the SDA to collect a PMWeb User's access requirements, i.e., the modules or areas of SDA PMWeb Systems that the user requests access to. The form must include proper justification of such need through the PMWeb User's supervisor. Submitted Technology Request Forms are reviewed for completeness and validated by the SDA Information Systems Division prior to implementing access to SDA PMWeb Systems.

New Project Setup Request Form – A form used by the SDA to collect all pertinent PMWeb User names and access requirements for both internal and external support staff. Submitted New Project Setup Request Forms are reviewed for completeness and validated by the SDA Information Systems Division prior to implementing access to SDA PMWeb Systems.

IV. Policy Provisions:

A. Authorization for PMWeb Systems Access

1. SDA PMWeb Systems contain sensitive data that must be protected from unauthorized disclosure or modification. In recognition of its responsibility to secure and safeguard this information, the SDA directs individuals that require access to PMWeb Systems for SDA business purposes to provide proper justification of such need through their supervisors. Such approval shall be based on one of the following justifications:
    a. An SDA employee requires access to the PMWeb Systems in order to perform work-related duties; or
    b. non-SDA Personnel require access to SDA PMWeb Systems in order to perform their SDA-related professional and/or contractual responsibilities.
2. Access will be provided through a PMWeb User Account, which shall be established only after a request for access has been submitted and approved in accordance with the Policy. The ability to grant approval to establish PMWeb User Accounts will be limited to the SDA Director of Information Systems, or their designee.
3. PMWeb User accounts shall be secured through the use of a username and a corresponding complex password. PMWeb User passwords are confidential information and are not to be shared. On a bi-annual basis, or upon the transfer of a PMWeb User to a different job function, the SDA will undertake an evaluation to determine whether, and to what extent, the PMWeb User bears a continuing business need for SDA PMWeb Systems access.

B. SDA PMWeb Systems Access Requirements

PMWeb Users are responsible for the security and protection of the information systems and/or database(s) of the SDA to which they have access. The physical and logical integrity of these resources must be protected against threats, such as unauthorized intrusions, malicious misuse and/or inadvertent compromise. In accordance with these security goals, the following rules shall apply without exception:

1. It is the responsibility of a PMWeb User to maintain the confidentiality of their SDA PMWeb access password, and not permit the use of their SDA PMWeb access username and password by others, whether by intent or negligence.
2. When accessing SDA PMWeb Systems through the use of personal computer equipment, or on any other device not owned by SDA, PMWeb Users are subject to the same usage and security rules and requirements set forth in the Policy Governing SDA Network Security or the Policy Governing SDA Network Access for non-SDA Personnel, as applicable to that PMWeb User.
3. The SDA Information Systems Division must ensure that SDA-owned computers used to access the SDA PMWeb Systems contain up-to-date Anti-Virus/Anti-Malware protection software.
4. As a condition for authorizing access to SDA PMWeb Systems, the SDA reserves the right to obtain personal information from a PMWeb User (e.g., name, address and/or telephone number), and further, may be required to release such personal information, pursuant to the requirements of the Open Public Records Act, or other applicable law or court order.
    a. Authorized individuals will not receive SDA PMWeb Systems access until they attend proper training, and may be required to attend follow-up SDA PMWeb Systems training.

C. Password Standards

The SDA uses passwords as a means for accessing its information systems and to authenticate system users.

The following standards establish the minimum requirements for password use and security, and shall be followed by all PMWeb Users, including system administrators assigned by the Director of Information Systems, or their designee:

1. Confidentiality: Stored passwords on the SDA Information System network or other SDA-issued equipment shall be classified as confidential data and must be encrypted. PMWeb User account passwords must not be divulged to anyone. A change of password shall be required when a PMWeb User is first assigned an account and each time a password reset is requested through the SDA PMWeb Systems or the Information Systems Help Desk. Passwords in readable form (e.g., written on paper) must be kept in a safe and secured location and not accessible to others. An example of a safe location is a locked drawer that is accessed only by the PMWeb User.
2. Minimum length: A password must be no fewer than twelve (12) characters, unless otherwise constrained by system requirements.

3. Composition: A complex password shall be required for all SDA PMWeb systems and must contain at least one capital letter and one special character such as an exclamation mark (!), at sign (@), caret (^), brace ({ or }), bracket ([or]) or comma.
4. Change and Reuse: Passwords must be changed at least every 90 days. When changing passwords, a PMWeb User will not be permitted to repeat use of a password that they used in any of their previous twenty four (24) successful password changes, as the system will reject the use of such attempted repeated password.
5. Lock-out features: To preclude password guessing, the SDA employs a lock-out feature to suspend a PMWeb User account after three (3) consecutive unsuccessful attempts to log on have been made. Assistance from the SDA Information Systems Helpdesk via phone (609-943-4500) or email at mishelpdesk@njsda.gov shall be required to unlock an account.

D. Requests for Activation of SDA PMWeb Systems Access

SDA Authorized Representatives shall submit requests for SDA PMWeb Systems access for their respective SDA employees through a fully-executed Technology Request Form and shall submit such requests for non-SDA Personnel in connection therewith through a fully completed New Project Setup Request Form. SDA Authorized Representatives shall submit such forms to the Division of Information Systems via (mishelpdesk@njsda.gov). The completed Technology Request Form must include details of projects and modules that the SDA Authorized Representative anticipates the proposed user will perform work on. SDA Authorized Representatives can also request activations through the SDA PMWeb Splash Page.

E. Request for Termination of SDA PMWeb Systems Access

A PMWeb User's SDA PMWeb Systems account will be deactivated upon an SDA Authorized Representative's written notice to the Information Systems Help Desk or the Director of Information Systems that the user's access to SDA PMWeb Systems is no longer required. The following are circumstances wherein a PMWeb User's access to SDA PMWeb Systems will be deactivated:

a. temporary or complete discontinuance of the PMWeb User's employment relationship with the SDA;
b. internal transfer of the PMWeb User within the SDA to a position that does not require continued access to SDA PMWeb Systems;
c. temporary or complete discontinuance of the PMWeb User's employment relationship with their employing agency or firm;
d. temporary or complete discontinuance of the employing firm's contract or assignment with the SDA; or
e. the duties or services provided by the PMWeb User no longer require continued access to SDA PMWeb Systems.

V. Responsibilities:

A. The **Director of Information Systems**, or their designee(s), shall:

1. Secure and protect SDA PMWeb systems and databases through infrastructure security applications, such as firewalls, Internet site filtering, anti-virus and network monitoring.
2. Ensure that the SDA Help Desk is adequately staffed during business hours to provide any needed detailed guidance to PMWeb Users on such matters as passwords, required forms and access to SDA PMWeb Systems.
3. Make arrangements for the activation of PMWeb User accounts upon receipt and approval of PMWeb User access requests.
4. Inform PMWeb Users of their obligation to abide by the Policy and other applicable departmental procedures developed to implement the Policy.
5. Work with technology service providers to repair or replace SDA-owned defective software and/or equipment.
6. Deactivate PMWeb User accounts and passwords when notified by an SDA Authorized Representative that a PMWeb User's access to SDA PMWeb Systems is no longer authorized or required.
7. Review PMWeb User accounts quarterly to ensure that such users have appropriate access to information systems and/or external networking connections and facilities.
8. Develop standard operating procedures, as necessary and appropriate.

B. PMWeb Users shall:

1. Protect electronic information resources to which they have access by not sharing SDA information with unauthorized persons, nor storing SDA information on computers which are not owned or managed by the SDA.
2. Protect passwords over which they have control and ensure that passwords provided to them are not shared with any person.
3. Change passwords when directed by the SDA PMWeb Systems in a prompt manner.
4. Immediately report the loss or theft of PMWeb User accounts or passwords to the Information Systems Help Desk via phone (609-943-4960) or email (mishelpdesk@njsda.gov).
5. Ensure that non-SDA devices used to access SDA PMWeb Systems have the latest version of virus and malware protection software.
6. Fully support the proper use of SDA PMWeb Systems by ensuring that all pertinent project information is entered into SDA PMWeb Systems so that information can be tracked as well as easily accessed.
7. Enter project-related information, updated project status, and/or update notes to the SDA PMWeb Systems within 2 business days of project-related events.

8. Ensure and validate that all data entered into SDA PMWeb Systems is accurate and factual.
9. Provide a complete, understandable explanation for any adjustments made in SDA PMWeb Systems by way of the SDA PMWeb Systems notes field or attached document(s) within 2 business days of the adjustment.
10. Acknowledge that they have read, understand and agree to comply with the Policy and the Policy Governing SDA Network Security or the Policy Governing SDA Network Access for non-SDA Personnel, as applicable to that PMWeb User, prior to receiving an assigned SDA PMWeb User account or password.

C. SDA Director-level employees and above, or their designee(s), shall:

Notify the Director of Information Systems, or their designee(s), that the SDA PMWeb Systems access of an individual managed by them is no longer authorized for SDA PMWeb Systems access due to any or the reasons described in Section IV. E.

VI: Procedures Particular to the Policy:

A. SDA PMWeb Systems Access Activation Process

1. Submitted SDA PMWeb Systems access requests are reviewed and validated by the SDA Information Systems Division prior to being fulfilled.
2. Before SDA PMWeb System access usernames and passwords are assigned by the SDA Information Systems Division to individuals who have been approved to access the SDA PMWeb Systems, such individuals must acknowledge that they have read, understand and agree to comply with the Policy and the Policy Governing SDA Network Security or the Policy Governing SDA Network Access for non-SDA Personnel, as applicable to that PMWeb User.

B. SDA PMWeb Systems Access Termination Process

1. SDA PMWeb Systems access termination notifications can be provided as follows:
   a. SDA Authorized Representatives shall use e-mail address (mishelpdesk@njsda.gov) to request that the Information Systems Help Desk disable the SDA PMWeb Systems accounts of PMWeb Users in connection therewith that no longer require continued access to SDA PMWeb Systems.
   b. Urgent requests may be provided via telephone to the Director of Information Systems, or their designee(s), followed by an email to (mishelpdesk@njsda.gov) supporting each request.
2. Information Systems Division staff members will commence disabling SDA PMWeb Systems usernames and passwords following SDA PMWeb Systems access termination requests and will create and use a PMWeb User termination checklist.

C. SDA PMWeb Systems Access Internal Transfer Process

1. Notification of a staff transfer can be provided as follows:

   The SDA Authorized Representative supervising a PMWeb User who is the subject of an internal transfer shall submit a Technology Request Form to the Information Systems Division to arrange for PMWeb User access rights consistent with the transferred employee's new Division and/or new responsibilities.

D. SDA PMWeb Systems Password Reset Requests

In instances when a PMWeb User needs to reset their SDA PMWeb Systems password for reasons such as the user forgot their password; the user suspects that their account has been compromised; due to loss or theft of the PMWeb User's account or password; or, for other security risk concerns, that user must contact the Information Systems Help Desk immediately via phone (609-943-4500) or email (mishelpdesk@njsda.gov). A temporary password will be issued to the PMWeb User and, if necessary, the Help Desk will assist the PMWeb User with changing their SDA PMWeb Systems password.

VII: References:

- Policy Governing Network Security (SDA Policy No. 1206)
- Policy for Network Access for Non-SDA Personnel (SDA Policy No. 1207)

VIII: Review Date: On an annual basis.

Supersedes Policy: IS-1208 dated November 24, 2014