Michigan Department of Health and Human Services (MDHHS)
MiSACWIS contract language for child caring institution (CCI) organizations
Revision Date: 11/30/2020

The Contractor shall ensure that applicable CCI staff has access to the Michigan Statewide Automated Child Welfare Information System (MiSACWIS) through a web-based interface, henceforth referred to as the "MiSACWIS application."

I. Federal and State Laws

The contractor shall comply with all federal and state laws regarding the use of computers and dissemination of information obtained from their use, along with any other applicable federal or state privacy and/or confidentiality laws, including but not limited to:

A. The Federal Information Security Management Act (FISMA) of 2002, 44 USC 3541 *et seq*.
B. The State of Michigan (SOM) Computer Crime Law (MCL 752.791 through MCL 752.797).
C. The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); HIPAA's implementing regulations, as amended, 45 CFR Parts 160-164.
D. The Patient Protection and Affordable Care Act of 2010, Public Law 111-148.
E. The Health Information Technology for Economic and Clinical Health Act of 2009, Public Law 111-5.
F. The Privacy Act of 1974, Public Law 93-579.
G. The Social Security Number Protection Act of 2010, Public Law 111-68.
H. The Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248.
I. Indian Child Welfare Act.
J. Internal Revenue Code, Public Act 114-38.
K. Identify Theft Protection Act, MCL 445.61 through MCL 445.79d.
L. Social Security Number Privacy Act, MCL 445.81 through MCL 445.87
M. Child Protection Law (CPL), MCL 722.621 through MCL 722.628.
N. Michigan Adoption Code, MCL 710.1 through MCL 710.70.
O. Family Educational Rights and Privacy Act (FERPA) of 1974.

II. General Provisions

The Contractor shall:

A. Require that MiSACWIS must only be accessed by users on a "work-issued" device, e.g., laptop, desktop, mobile device, etc., and must read and adhere to the State of Michigan Department of Technology, Management and Budget (DTMB) Policy 1340.00.130.02 Acceptable Use of Information Technology: https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf
B. Enroll each staff with responsibility for information input in the MiSACWIS application by completing an access request in the Database Security

Application (DSA) which is the electronic access management system for MiSACWIS.

C. Comply with all terms and conditions that MDHHS establishes regarding the Contractor's use and access to the MiSACWIS application.
D. Allow access to MiSACWIS by state- and federal-agency staff for the purposes of an audit or other necessary evaluations.
E. Designate at least one, but no more than three authorized requestors.
F. Identify at least one MiSACWIS liaison to relay vital MiSACWIS information to MiSACWIS users. The director or designee can email the liaison's name, email address, agency/organization name, address, and telephone number to the MiSACWIS team at MiSACWIS@michigan.gov.
G. Within 24 hours, report all changes to MDHHS (e.g., a new authorized requestor, locations, license number, etc.) by contacting the Office of Child Welfare Policy and Programs (OCWPP) contract analyst.
H. Agree to accept financial responsibility for any costs accruing to the State of Michigan as a consequence of a data breach by the Contractor and/or the Contractor's employees and/or subcontractors.
I. Use the MiSACWIS application to validate the Contractor's payment roster for board and care payments.
J. Use the MiSACWIS application in accordance with MDHHS contractual requirements and policy manuals.
K. The Contractor agrees that the MiSACWIS application roster approver is not a caseworker or a direct-care supervisor.

III. Authorized Requestor (AR)

The authorized requestor (AR) shall:

A. Submit a MiSACWIS access requests in DSA identifying him/herself as the authorized requester.
B. Review and approve all MiSACWIS access requests in DSA for foster care and adoption social services staff.
C. Maintain a copy of all DHS-815 requests used to request access prior to transitioning to DSA.
D. Monitor user access for the agency quarterly by reviewing the MiSACWIS user sign-on report and user group audit report. Submit monitoring reports as requested by MDHHS.
E. Notify MDHHS Application Security via email at MDHHS_Application_Security@michigan.gov
    1. Within 24 hours of a MiSACWIS user's departure from employment. Staff departures include any extended leave of absence, which is defined as absent for more than two weeks.
    2. Immediately for users who are terminated for cause.
F. Notify MDHHS upon discovery of a possible:
    1. Unauthorized use or access to MiSACWIS.
    2. Instance of misdirected, unpermitted, or unauthorized communications or breaches that contain sensitive or protected heath information (PHI)

information (reference Administrative Policies Legal (APL) 68D-102 Physical Safeguards for the Storage, Use or Disclosure of PHI.)
3. Disclosure of confidential/private information, including a breach by an employee or contractor, or any other person.

G. The AR must work with the individual who made an observation or received information about a breach. Within 24 hours, the AR and/or the individual must complete the following activities:
   1. Take appropriate steps to contain the incident, if still in process.
   2. Complete the *Incident Reporting Form* (DCH-1422) as fully as possible and email it to MDHHSPrivacySecurity@michigan.gov.

H. Establish policy consistent with the SOM security policies that are distributed to all MiSACWIS users, along with the provision of security awareness training and documentation of the training attendance. The authorized requester may make the identified SOM policies available to employees, or the Contractor may have a written security policy. The written policy may be more restrictive than the SOM policies, but the policy must meet the minimum requirements outlined in the SOM policies. The policies shall:
   1. Prohibit the sharing of authentication information, e.g., user IDs, passwords, and PINs.
   2. Limit users' MiSACWIS access to authorized users.
   3. Limit users' access to MiSACWIS on a "work-issued" device, e.g., laptop, desktop, mobile device, etc.
   4. Prohibit unauthorized people from viewing MiSACWIS information.
   5. Include a user's agreement to protect the sensitive and confidential information in MiSACWIS (this can be accomplished by the user submitting an access request in the DSA).
   6. Require that Health Insurance Portability and Accountability Act's (HIPAA's) privacy and security rules are communicated and enforced, and that users are properly trained and informed of their responsibilities.
   7. Address the requirements for secure document handling identified below.
   8. Require all users of the MDHHS automated systems to read and agree to comply with:
      a. Acceptable Use of Information Technology Standard 1340.00.01 at: https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf
      b. Services Requirements Manual (SRM) 131 *Confidentiality*.
      c. MiSACWIS Privacy Policy.
      d. MiSACWIS Michigan Usage Agreement.
   9. Be consistent with the SOM policies identified below:
      a. 1340.00.110.03 Storage of Sensitive Information on Mobile Devices and Portable Media Standard https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/IT%20Policies/1340.00.110.03%20Storage%20of%20Sensitive%20Information%20on%20Mobile%20Devices%20and%20Portable%20Media%20Standard.pdf

b. 900.02 Access Control
https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/Policies/900.02%20Access%20Control.pdf
c. 100.20 Security Breach Prevention and Notification Requirements
https://stateofmichigan.sharepoint.com/teams/insidedtmb/work_/policies/Policies/100.20%20Security%20Breach%20Prevention%20and%20Notification%20Requirements.pdf
d. 1340.00.130.02 Acceptable Use of Information Technology
https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf

IV. Document Handling

The Contractor shall:

A. Require that confidential documents, forms, and negotiable documents must be stored, controlled, and periodically inventoried.
B. Require that MiSACWIS documents are handled and retained in accordance with applicable federal, state, and local laws, orders, directives, and MDHHS policies.
C. Require that erroneously created confidential information must be shredded or otherwise destroyed.
D. Store confidential documents in MiSACWIS. If the documents are download to the user's computer or the agency's internal network, the organization must comply with encryption requirements per Federal Information Processing Standard (FIPS) Publication 140-2.
E. Confidential documents must not be stored in the cloud, e.g., One Drive, SharePoint, DropBox, Google Drive, Box.
F. Comply with SOM encryption standards for data in flight related to the transmission of confidential or sensitive documents or information.
G. Ensure that sensitive or confidential information never be included in an email subject line.
H. Ensure that sensitive or confidential information never be included in the body of an email unless encrypted.
I. If confidential documents are printed, they must be stored in a locked cabinet. Once the printed document is no longer needed, the document must be shredded to meet IRS standards.

V. Desktop and Laptop Standards

A. The contractor shall apply the applicable IRS computer security configurations/desktop standards, which are required to be applied to the employees' workstations. These documents include:
   1. Internal Revenue Service Office of Safeguards, SCSEM Subject: Microsoft Windows 7.
   2. Internal Revenue Service Office of Safeguards, SCSEM Subject: Microsoft Windows 8.

3. Internal Revenue Service Office of Safeguards, SCSEM Subject: Microsoft Windows 10.
4. Internal Revenue Service Office of Safeguards, SCSEM Subject: MACOSX 10.11 and 10.12.

The most recent versions of these documents can be found at: http://www.irs.gov/uac/Safeguards-Program.

B. The Contractor shall use a supported web-browser for accessing the MiSACWIS application that supports 128-bit transport layer security (TLS) encryption, which is regularly updated with any necessary security patches. MiSACWIS-supported browsers include:
   - Microsoft Edge
   - Chrome
   - Firefox
   - Safari
C. The Contractor shall have a currently supported operating system and all application software must be patched for vulnerabilities on a regular basis as required under applicable state and federal regulations.
D. The Contractor shall have virus protection software that performs an automatic/scheduled full-system scan at least monthly for malicious code and automatically updates its signatures. The virus software must automatically scan for critical software updates and security patches and install them.

VI. Mobile Device (including laptops and tablets) Standards

A. The contractor shall comply with the mobile device standards outlined in the IRS Publication 1075, and the Centers for Medicare and Medicaid Services (CMS) polices.
B. The contractor shall, at a minimum, ensure that cellular wireless devices:
   1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing.
   2. Are configured for local device authentication.
   3. Use advanced authentication.
   4. Encrypt all confidential documents on the device.
   5. Erase cached information, to include authenticators in applications, when session is terminated.
   6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the Organization level.
   7. Employ antivirus software or run an MDM system that facilitates the ability to provide antivirus services from the Organization level.
C. If implemented, the contractor must ensure the MDM is in compliance with IRS and CMS MDM requirements.

VII. Wireless Connections

The Contractor shall ensure wireless connections within their office comply with current IRS and CMS security requirements.

VIII. Media Disposal

The contractor shall meet the minimal IRS requirements prior to the media being surplused, transferred, traded-in, disposed of, or the hard drive being replaced. This standard requires proper disposal, transfer, or destruction of state information contained in removable, portable, or installed media containing protected data. This standard requires proper disposal, transfer, or destruction of state information contained in removable, portable, or installed media containing protected data.

IX. Training

A. The Contractor shall ensure that all staff with access to the MiSACWIS application complete both the MDHHS Security Training and MDHHS Privacy Training in the Learning Center prior to accessing MiSACWIS. The MDHHS Security Training and MDHHS Privacy Training are required to be completed by all staff annually or as required by MDHHS to maintain system access.
B. The MiSACWIS application roster approvers are required to complete the MiSACWIS Roster Verifier computer-based training (CBT).
C. The Contractor shall maintain training documentation, which verifies completion of required MiSACWIS application training for each staff person.