NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

| Office of Information Technology Services Policy | **No:** ITS-P21-004 |
|---|---|
| **ITS Policy**: **Local District Social Services Access to State Applications** | **Issued:** 07/27/2021<br>**Issued By:** NYS Office of Information Technology Services<br>**Owner:** Chief Technology Office |

## 1.0 Purpose and Benefits

The State provides county local social services districts (LDSS) access to the New York State (NYS) welfare management system and other applications associated with the Office of Children and Family Services (OCFS), Office of Temporary and Disability Services (OTDA), and the Department of Health (DOH).

This policy establishes a modern and more secure operating model for providing LDSS employees with access to State applications and providing the LDSS with government-to-government (G2G) access to data supporting LDSS operations.

## 2.0 Authority

*Section 103(10) of the State Technology Law* provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish Enterprise Information Technology (IT) Policies, Standards and Guidelines.*

## 3.0 Scope

This policy document applies to ITS employees, contractors, and consultants; OCFS; OTDA; DOH; and the LDSS.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002, and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011, and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

# 4.0 Information Statement

The State provides several core service delivery functions to the LDSS to support access to the welfare management system:

- Workplace User Experience;
- User Identity and Access Services, including privileged access;
- Network Services; and
- Security and Data Access.

## 4.1 Workplace User Experience

### 4.1.1 Virtual Desktops

Virtual Desktops are pooled, Windows desktops, hosted in the ITS managed Excelsior Cloud which provide consistent, secure access to State-managed applications. LDSS employees may access Virtual Desktops from a State-managed, county-managed, or other network with access to the internet using an appropriately configured personal computer, thin client, or mobile device which supports the Virtual Desktop service or a supported web browser.

Virtual Desktops will include access, as appropriate, to State applications directly supporting LDSS functions; required third party applications and licensing; and State networks and services. Virtual Desktops will not include access to networks or applications specific to any single LDSS entity or not specifically required for LDSS access to State applications.

### 4.1.2 Multi-Factor Authentication

Access to Virtual Desktops, Virtual Private Network (VPN), third party applications, or other systems requires that each LDSS employee use a State-managed user credential and associated multi-factor authentication (MFA) device. MFA is available either as a physical token or smartphone application and is provided by the State.

### 4.1.3 Credentials and File Hosting

The State will continue to provide credentials necessary to access State applications and associated services to LDSS employees.

Data germane to the normal and customary use of State applications, stored on State-managed file servers supplied by the State, will be migrated to centralized storage in the ITS-managed Excelsior Cloud.

The State will not support components including file/print servers and endpoint management servers.

### 4.1.4 Print

Virtual Desktop Printing will be delivered using a software-based service that securely transports data through the encrypted Virtual Desktop session before forwarding to locally attached or networked printers.

## 4.2 User Identity and Access Services

LDSS employees accessing State systems must use individual State-provided credentials in State-managed identity systems, consistent with applicable security policies. Shared credentials are not permitted.

Privileged or administrator access to State systems, including managed desktops or servers on the State network, require that LDSS employees agree to undergo fingerprint-based background checks and submit to annual compliance training. The State will bear the cost of fingerprinting. The LDSS must ensure that staff complete training mandated by OTDA, OCFS, DOH, or any other applicable government agency, as necessary to comply with requirements for access to regulated data.

All privileged access will be facilitated by a State privileged access management system.

## 4.3 Endpoint Devices

Individual LDSSs are responsible for providing their employees with appropriate endpoint devices to access State applications using Virtual Desktops. As the existing devices were procured with non-State funds, ownership of existing endpoint devices will be assumed by each respective LDSS.

### 4.3.1 Device Maintenance and Support

Active legacy devices on the State's inventory list as maintained by the State will continue to be maintained by the State through their service lifecycle, but not later than January 10, 2023. Devices determined to require maintenance will be replaced by new or refurbished equipment. These replacement devices may include manufacturers warranties but will not include additional maintenance provided by the State and the devices will not be added to the State's inventory list.

Devices provided to facilitate remote work and utilization of Virtual Desktop technology will not be added to the State's inventory list. These devices include manufacturer warranties. The State will not provide maintenance or support services and ownership of the devices will devolve to the counties.

### 4.3.2 High Speed Printers

The State will continue to support and maintain welfare management system High Speed Printers.

## 4.4 Network Services

### 4.4.1 County Network Access Point

The State will provide connectivity to network access points based on operational or engineering needs. To facilitate the migration to Virtual Desktop delivery, the State will upgrade circuits and other networking components as appropriate to provide support for Virtual Desktop operations.

#### 4.4.2 State Managed Firewall

The State will continue to maintain the OneNetNY solution to support interconnectivity between State and LDSS systems.

#### 4.4.3 Virtual Private Network

The State will provide secure network access to State managed laptops through their service lifecycle, but not later than January 10, 2023.

The State will continue to provide secure remote access to LDSS employees using Virtual Desktops.

### 4.5 Security and Data Access

#### 4.5.1 Security Compliance

Under the authority of *State Technology Law Section 103 (10)*, ITS formulates security policies that apply to all third parties, including local governments, that use or access any IT resource for which the state has administrative responsibility. LDSSs will be expected to comply with all Statewide security policies, including but not limited to the Acceptable Use of Information Technology Resources Policy. In instances where compliance is not possible, security exceptions must be filed in accordance with the Information Security Exception Policy to ensure proper understanding of risk and the creation of a corrective action plan.

#### 4.5.2 Publicly Accessible Computers

To maintain the State's security posture, computers, kiosks, or other devices directly accessible to the public must not be connected to any internal NYS network and should not be connected to any County active directory domain.

#### 4.5.3 Local County Applications

To improve the State's security posture and facilitate State and county compliance requirements, county-specific applications cannot be on State-managed networks.

The State will provide clear delineation between State and county-supported applications. County applications must be capable of running on current, supported application platforms including, but not limited to, operating systems and web browsers.

#### 4.5.4 Access to Data for County Processing Needs

The State, in support of partner agencies (OCFS, OTDA and DOH), will provide data to support county operations with methods consistent with operational needs and in compliance with all Federal and State security policy requirements.

## 5.0 Compliance

This policy document shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

In order to provide sufficient time for each LDSS to establish procedures and systems to comply with this policy, the State shall provide a period of transition not to exceed January 10, 2023. All new devices and systems implemented after this policy's publication date must be in compliance with all provisions of this policy.

## 6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

## 7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

**Chief Technology Office**
**Reference: ITS-P21-004**
**NYS Office of Information Technology Services**
**State Capitol, P.O. Box 2062**
**Albany, NY 12220**
**Phone: (518) 402-7000**
**Email: CTO@its.ny.gov**

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

## 8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in *NYS-P09- 003 Process for Establishing Information Technology Polices, Standards and Guidelines.*

| Date | Description of Change | Reviewer |
|---|---|---|
| 07/27/2021 | Issued policy | Chief Technology Office |

## 9.0 Related Documents

ITS Security Policies