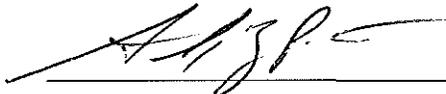


**Office of Management and Enterprise Services
Information Services Division**

Policy Title: OMES ISD Local Administrator Account Policy

Effective Date: October 21, 2013

Pursuant to 62 O.S. §§34.11.1 and 34.12, the above-referenced policy, a copy of which is attached hereto, is established and adopted by the Information Services Division of the Office of Management and Enterprise Services.



Alex Z. Pettit, Chief Information Officer

10.22.13
Date



OMES ISD LOCAL ADMINISTRATOR ACCOUNT POLICY

Effective Date of Policy: October 21, 2013	Next Scheduled Review: Two years
Prior Policy: N/A	Policy Number: ISD DS5.4.1
Last Reviewed: N/A	Replaces Policy Number: N/A
Date Policy Last Revised: N/A	
Approved: Alex Pettit, Chief Information Officer	Approval Date: October 21, 2013

Statutory Reference: Title 62 of the Oklahoma Statutes

Pursuant to 62 O.S. §§34.11.1 and 34.12, the Information Services Division (“ISD”) of the Office of Management and Enterprise Services (“OMES”) is responsible to direct the development, implementation and management of appropriate standards, policies and procedures to ensure success of state information technology initiatives and to establish and enforce minimum mandatory standards for information security and internal controls. Such authority and responsibility is critical to the mission of ISD set forth therein. Accordingly, this Local Administrator Account Policy applies to all OMES ISD employees, wherever located. Violation of this Policy may result in revocation of administrative privileges and possible disciplinary action, up to and including termination.

The consolidation of information technology infrastructure, data and, computer systems presents unique possibilities and challenges for the State of Oklahoma. As a result of this consolidation effort, a new advanced information ecosystem has developed that requires new approaches to cybersecurity. The impact to citizens, the economy of Oklahoma and the nation depend on the cybersecurity posture of the State’s information technology infrastructure and computer systems. A poor or mismanaged cybersecurity posture could compromise the entire State information ecosystem. The threats are very real. Attacks such as malicious code attacks, directed attacks by hackers, and foreign governments, Advanced Persist Threats, criminal enterprise, espionage, and employee misconduct have advanced to the realm of technically proficient attackers and those with the motivation to succeed at all costs.

The State Information Security Policy, Procedures and Guidelines do not allow for local administrator access by users or super users. When an exception is requested, a risk review is conducted to determine whether, and to what extent, such an exception is justified to grant local administrator access to an individual. The job roles and responsibilities must be defined if administrative privileges are needed to accomplish State or agency mission and support business functions. When users are granted a local administrator account, the following additional responsibilities apply:



**State of Oklahoma
Office of Management &
Enterprise Services
Information Services Division**

Local Administrator
Account Policy

-
- Employees must NOT use the local administrator account to browse the web (unless directly for the correction or facilitation of assigned work duties).
 - Employees must NOT use the local administrator account as a normal login for daily systems use; the account shall be used only for items that need administrative level access to correct issues or resolve problems.
 - Employees must NOT use the local administrator account to change or modify any portion of the systems to bypass or circumvent security controls and all usage as a local administrator account must be in accordance with this Policy as well as the State Information Security Policy, Procedures and Guidelines Section 5.3 Personal Computer Usage and Section 5.4 Email Usage, as amended.
 - Employees must NOT install unapproved software on State owned assets and must follow current established procedures for permission to install software through the OMES ISD Service Desk.
 - Employees must NOT install personal applications on State owned assets – “Free” software is not free. The tracking and usage that is taken from the systems violates state confidentiality and privacy laws and could lead to a compromise of State and Federal data.

Periodic audits of local administrator account activity will be conducted by the OMES ISD Security Department Compliance Manager and prompt and full cooperation is expected of OMES ISD employees in connection with such audits.