

Security Risk Management Framework

Tiered Security Risk Management Approach

Tier 1

Organizational (Governance)

- **IT Governance Committee**

Members

AA&R – Dan Evans

Area Superintendent - Bob Poth

CTAE, Mark Hunt

Deputy Superintendent – Bill Corbett

Digital Learning – Connie Kolosey

Finance - Kevin Smith

Maintenance - Clint Herbic

Student and Community Services – Lori Matway

Teaching & Learning – Kevin Hendrick

TIS - Tom Lechner

- **School Board Policies**

1281 – Use of Employee’s Personal Property at Work

2540 – Use of Multi-Media

3213.01 – Communications with Parents and Students via Electronic Media

5500 – 5500.13 – Code of Student Conduct

7530 – Lending of District-Owned Equipment

7530.01 – Staff Use of Electronic Communication Devices

7540 – Computer Technology and Networks

7540.02 District Web Page

7540.03 – Network/Internet Acceptable Use Agreement

7540.04 – Use of Electronic Resources – Acceptable Use Agreement

- **TIS Security Council**

Members

Ceneskie, Robert, Senior Instructional User Support Analyst

DiLeonardo, David, Director, Application Support and Development

Doughty, Brian, Network Administrator

Heeren, Alex, Digital Learning

Kelly, Casey, Computer Support Analyst, Network and Telecommunications

Hartwell, Diane, Systems Administrator

Johannesen, Michael, Manager User Support

Kelly, Casey, Network Admin. Apprentice

Lechner, Thomas, Assistant Superintendent, Technology and Information Systems

Maliszewski, Mark, Database Administrator

Ken Bonnell, Supervisor, Help Desk

Paske, Robert, Manager, Core Systems

Wilder, Paul, Senior User Support Analyst

Tier II

Mission/Business Process
(Information and Information Flows)

- Microsoft Health Check – July 2018
See reports
- PCS Internal Scans – 2018-19

Tier III

Information System
(Environment of Operation)

- District Strategic Goals
 - Goal 7.2 – Computer Based Testing (CBT)
 - Goal 7.3 – Purchase new ERP
 - Goal 7.4 – Upgrade Wireless Network
 - Goal 7.6 – IT Governance
- TIS Policies and Procedures
 - Risk Management Framework
 - Password Procedures
 - Incident Response Plan
- PCS Forms
 - PCS Form 2-2695 – Network/Internet Acceptable Use Agreement
 - PCS Form 3-1943 – Property Removal
 - PCS Form 3-3160 – Equipment Assignment List