Section 11: Bibliography

Minnesota: Guidelines and Reports

Office of the Secretary of State.
Digital Signature Program (including proposed “Minnesota State Agency Digital Signature Implementation and Use Standard”). 1999.
[ http://www.sos.state.mn.us/business/digital/gl.html ]

Office of the Legislative Auditor.
Summaries of the following reports are offered at: http://www.auditor.leg.state.mn.us/

need for comprehensive security program; formal systems development standards and systems security tests; security standards for wireless technologies; periodic scans for unauthorized wireless access points; documentation of access control standards; access in line with employee duties; no sharing of accounts and passwords; use of complex passwords; procedures for promptly installing security-related patches; need to define security events to log; regular review of security logs; periodic system scans for known security weaknesses

need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties

need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties

need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties

need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties
  {need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

  {need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

  {need for review of access to systems; need to restrict access to systems}

  {separation of incompatible duties and security clearances; access in line with employee duties}

  {need for comprehensive security program}

  {access in line with employee duties; separation of incompatible duties and security clearances}

  {password management; access in line with employee duties; audit trails for individuals}

  {separation of incompatible duties and security clearances; access in line with employee duties; restriction of access to private data}

  {separation of incompatible duties and security clearances}

{development and documentation of formal data extraction standards and procedures; periodic information technology risk assessments; development of detailed system security baselines; independent assessment of security controls; separation of incompatible duties and security clearances}

{need for comprehensive security infrastructure; active management of systems; periodic testing and validation of controls; separation of incompatible duties and security clearances; access to data from uncontrolled environments and interfaces; access in line with employee duties; password management; audit trails for individuals}

{separation of incompatible duties and security clearances}

{periodic review of appropriateness of security clearances}

{need for records retention schedule}

{need for comprehensive security infrastructure addressing current information technology risks}

{need for periodic information technology risk assessments; need to develop detailed system security baselines; independent assessment of security controls; need to develop standard access request protocols; timely review of security clearances; password management; audit trails for individuals; access in line with employee duties; control of network access points; review systems for unnecessary and insecure services; prompt installation of security-related patches; ongoing monitoring of systems for security-related events}

{access controls for computer program libraries}
{password and account management; access controls for computer program libraries}

{No major weaknesses were identified.}

{timely review of security clearances; access in line with employee duties; formal standards and procedures for access; access controls for mission-critical systems; password management; monitoring of security-related events; encryption during file transmission}

{timely review of security clearances; access in line with employee duties; unique user accounts}

{timely review of security clearances; access in line with employee duties}

{timely review of security clearances; access in line with employee duties; unique user accounts}

{need for a comprehensive security infrastructure; written documentation of security policies, procedures, and standards}

{timely review of security clearances; access in line with employee duties; unique user accounts; password control}

{documentation of system design; cross-training of computer staff}

{timely review of security clearances; access in line with employee duties; procedures; written documentation}

{lack of comprehensive security program leading to numerous weaknesses}

{access in line with employee duties}

{timely review of security clearances; access in line with employee duties}

{timely review of security clearances; access in line with employee duties; procedures; written documentation}

{access in line with employee duties; encryption during file transmission}

{access in line with employee duties; access controls to mission-critical programs; information technology risk assessment}

{access in line with employee duties}

{access in line with employee duties}

{timely review of security clearances; access in line with employee duties}
{timely review of security clearances; access in line with employee duties; procedures; written documentation}

{timely review of security clearances; access in line with employee duties; procedures; written documentation}

{timely review of security clearances; access in line with employee duties; written documentation}

{lack of comprehensive security program; written documentation}

{lack of training}

{access in line with employee duties}

{access in line with employee duties; password control}

{timely review of security clearances; access in line with employee duties}

{system-development planning; formal risk assessment; timely review of security clearances; access in line with employee duties; password control; physical environment; security incident detection and response; written documentation of system, standards, policies, and procedures}

{accuracy of records}

{periodic review of system security; timely review of security clearances; access in line with employee duties}

{access in line with employee duties; written documentation}

{access in line with employee duties; written documentation}

{timely review of security clearances; access in line with employee duties}

{access in line with employee duties}

{access controls; disaster recovery plans; system backups}

{written system documentation}

{timely review of security clearances; access in line with employee duties}

{access in line with employee duties}

{formal risk assessment; timely review of security clearances; access in line with employee duties; security policies and procedures}

{timely review of security clearances}

Financial-Related Audit: Department of Administration InterTechnologies Group,
{timely review of security clearances; access in line with employee duties; written
documentation}

Financial-Related Audit: Department of Finance, Information Warehouse Data Integrity
{access in line with employee duties; password controls}

Financial-Related Audit: Minneapolis Community and Technical College, July 1, 1996,
{access in line with employee duties; unique users IDs and passwords}

Financial-Related Audit: Alexandria Technical College, July 1, 1996, through December
{access in line with employee duties; records retention policies, documentation,
and training}

Financial-Related Audit: Lake Superior College, July 1, 1996, through December 31,
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Pine Technical College, July 1, 1996, through December 31,
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Departments of Commerce and Public Service, July 1, 1996,
{system audit trails}

Financial-Related Audit: Minnesota State University Moorhead, July 1, 1996, through
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Dakota County Technical College, July 1, 1996, through
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Normandale Community College, July 1, 1996, through
{access in line with employee duties; control of user IDs}

Financial-Related Audit: Public Utilities Commission, July 1, 1997, through December


Trustworthy Information Systems Handbook

{security procedures; access controls; written documentation; disaster recovery plan}

{formal risk assessment; timely review of security clearances; password control; written documentation of system, policies, and procedures}

{timely review of security clearances; access in line with employee duties; unique users IDs and passwords}

{data integrity and security; procedures}

{timely review of security clearances}

{timely review of security clearances; access in line with employee duties; security administration; security procedures and documentation; disaster recovery plan}
{quality control; security administration; written documentation; user training; disaster recovery plan}

{transaction history files; access in line with employee duties; unique user accounts; disaster recovery plan}

{timely review of security clearances; access in line with employee duties}

{security administration; security policies; timely review of security clearances; access in line with employee duties; external systems}

{access control; timely review of security clearances; access in line with employee duties; system documentation}

{transaction history files; access in line with employee duties; disaster recovery plan}

{access control; clearance in line with employee duties}

Minnesota Department of Administration, Office of Technology.
The following reports are available at http://www.ot.state.mn.us/standards.


[ http://www.mnhs.org/preserve/records/electronicrecords/erguidelines.html ]

**Minnesota: Laws**

[ http://www.revisor.leg.state.mn.us/ ]

[ http://www.revisor.leg.state.mn.us/stats/13/ ]

*Chapter 15.10 (Records Delivered to Department Heads).* Statutes. 1998.
[ http://www.revisor.leg.state.mn.us/stats/15/10.html ]

*Chapter 15.17 (Official Records).* Statutes. 1998.
[ http://www.revisor.leg.state.mn.us/stats/15/17.html ]

[ http://www.revisor.leg.state.mn.us/stats/138/163.html ]

*Chapter 138.17 (Government Records; Administration).* Statutes. 1998.
[ http://www.revisor.leg.state.mn.us/stats/138/17.html ]

[ http://www.revisor.leg.state.mn.us/stats/325K/ ]

*Chapter 325L (Uniform Electronic Transactions Act).* Statutes. 2000.
[ http://www.revisor.leg.state.mn.us/forms/getstatchap.shtml ]

[ http://www.revisor.leg.state.mn.us/arule/8130/7500.html ]

*Chapter 8275 (Secretary of State: Electronic Authentication).* Rules. 1998.
[ http://www.revisor.leg.state.mn.us/arule/8275/ ]

**Other States: Guidelines, Reports, and Laws**


Federal Government: Guidelines, Reports, and Laws


U.S. Department of Defense.


International Government: Guidelines, Reports, and Laws


National Organizations: Guidelines and Reports

Association for Information and Image Management.
The following reports are available for purchase at: http://www.aiim.org


[ http://www.isaca.org/cobit.htm ]


[ http://www.law.upenn.edu/bll/ulc/ulc_frame.htm ]

Nuclear Information and Records Management Association.
The following reports are available at: http://www.nirma.org


Electronic Records Projects and Studies


University of Pittsburgh, School of Information Sciences. *Functional Requirements for Evidence in Recordkeeping*. 1996.