

## **e-Diagnostics Security Guidelines V1.1**

### **Purpose/Scope:**

Define Information Technology security guidelines to support e-Diagnostics as defined in the International SEMATECH e-Diagnostic Guidelines. All guidelines apply to individual factory tools as well as any intermediate storage or concentration areas. Intellectual property protections, such as recipe content are addressed by the e-diagnostics team and are beyond the scope of this document.

1. System, including security, must be based on non-proprietary networking and computer architecture.
2. System must meet or exceed standard Information Technology security practices, as defined in ISO 17799.
3. Communication must take place over standard communication connections using TCP/IP protocols. Legacy serial connections may be used for low bandwidth tools.
4. All remote access must be from only known identifiable sources using techniques such as PKI digital certificates validated by an agreed certificate authority, handheld authenticators or biometric techniques.
5. Data transmission and external storage must have the capability to be encrypted using standard publicly available secure methods in compliance with export control restrictions. All Internet and Extranet based remote access and storage must be secure and encrypted. Intranet based remote access and storage is at customer discretion.
6. Audit trails, including who, what and when must be maintained for all data transfers and any remotely initiated changes.
7. System must support detailed access control at the data item level for read, write, and remote control functions.
8. System must function as part of a single network connection to the tool. It must also be capable of being supported on a separate dedicated network if desired. Security requirements apply to multiple networks if used.
9. Data transmission volumes and requirements must be clearly defined for normal and maximum levels.
10. Firewall configuration impact must be minimal and clearly defined.