



# IT Security Policies

---

Jeff Jackson  
jjackson@nasb.com

1



## Written policies — the foundation of your IT Security

- Every institution should have written IT security policies regardless of asset size or degree of implemented technology

2



## Benefits of written policies

- Improved security
- Appropriate behavior defined
- Lays groundwork of what tools and procedures needed to implement
- Enforcement
- Audit
- Documentation for H/R issues

3



## Design

- Designate a project leader
- Assemble development team if needed
- Decide on policy goals and scope
- Balance control with productivity
- Large comprehensive document or several smaller, more specific documents

4



## Some policies to consider

- Acceptable use
- Antivirus
- Password protection
- Risk assessment
- Audit
- Server security
- Intrusion Detection

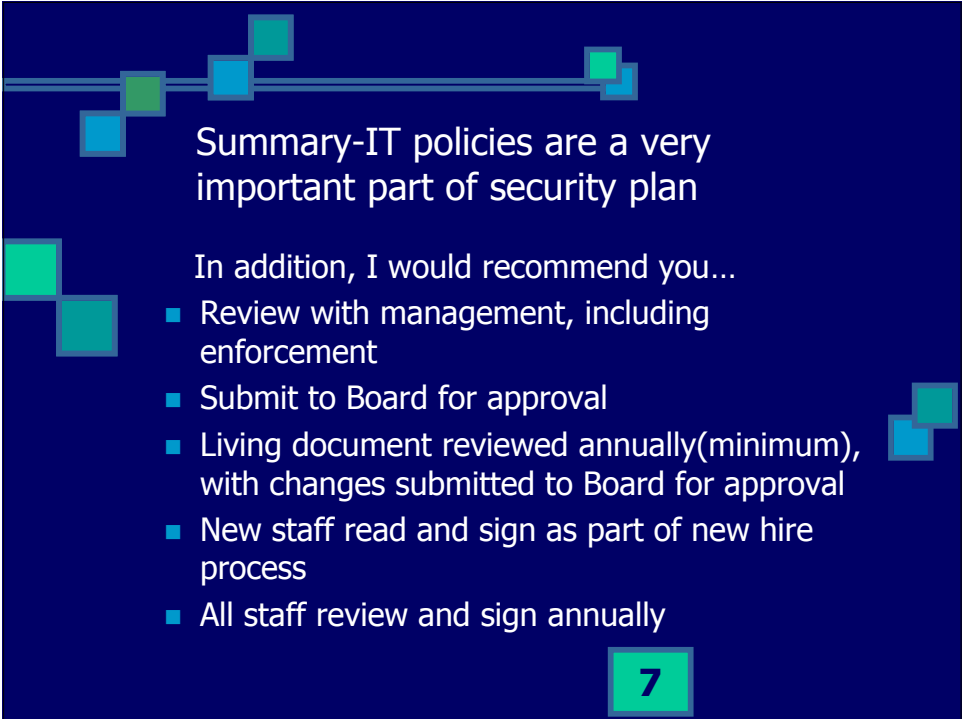
5



## Other policies if applicable

- Wireless communication
- Remote access/VPN/ ISDN/dial-up
- Acceptable Encryption
- Application service standards
- Electronic mail
- Information Protection
- Perimeter security

6



Summary-IT policies are a very important part of security plan

In addition, I would recommend you...

- Review with management, including enforcement
- Submit to Board for approval
- Living document reviewed annually(minimum), with changes submitted to Board for approval
- New staff read and sign as part of new hire process
- All staff review and sign annually

7



Some Web resources

<http://www.sans.org/>  
<http://www.ietf.org> (refer to RFC 2196)  
<http://csrc.nist.gov/>

8