ACROSS THE
STATES BANK

3/31/2024

ORGANIZATIONAL IT SECURITY POLICY

Liela Pressley ITT-380 Information Assurance

Professor Christopher Molstad

TABLE OF CONTENTS

OUR POLICY SUMMARY

All parties must adhere to the IT security policies and practices relevant to their processes as it is essential to being proactive in security awareness, risk miitgation and threat analysis.

By being aware of the company’s assets and software not only allows our company to priortize where to allocate security efforts and reosurces but promotes a culture where we all strive towards the common goal of building Across the States Bank to success in all areas.

ASSET MANAGEMENT & DISCOVERY

CONTROLS- ASSIGNING RESPONSIBILITIES

1. Identify and record important info about assets (location, license info, security classificaiton or categorization). This will ensure movement/changes to assets is documented/updated.
2. Each asset needs an assignd owner to be responsibile fo rthe security of the asset and has ulitmate accountability for proper classification and reviews authorizations of use- this can be delegated but responsibilities are still with the owner.
3. Each department will collaborate and develop a policy/guidelines for acceptable asset use that makes the most secure sense. This must be endorsed by senior managment and require elaboration on rules and responsibilities of asset usage by internal and external parties.

INFORMATION ASSET CLASSIFICATION

Organizing information according to valu or impact to organization is necessary for allocating resources cost-effectively towards enforcing confidentiality, integrity and availability efforts on assets.

Classifcation Guidelines:

- Identify asset/information owners and involve their input
- Seek professional legal advice on business, legal, and industry requirements
- Information orginator is responsible for classifying and protecting it based on policy/procedures
- Ensure that classifcations occur regularly, taking into account its life cycle and authorized individuals to access it.
- Ensure proper labels of confidentiality on all labels such as: secret, restricted, public and/or processing, transmission, storage and disposal.

RISK ASSESSMENT

Risk management planning is essential to reducing overall organizational risk in a constantly changing environment and with constantly changing information/risk.

By implementing policies, procedures, and practices to identify risk events Across the States Bank can effectively identify, analyze, treat, evaluate, and continue to improve risk management.

FORMING THE ASSESSMENT

1. Establish the aim, scope and boundaries as the foundation
2. Establish risk evaluation criteria to determine acceptable levels of risk
   a. based on: operational, technical, financial, legal, social, humanitarian, etc
   b. utilize standard threat profiles (STP) depending on typical threats
3. Consult with experts in specific threats/industry
4. Observe actual events and incidient within relevant industrial spaces.

Risk Matrix

impact

	low	medium	high
high	low	med	high
medium	low	med	med
low	low	low	low

likelihood

RISK TREATMENT

There are about 5 different levels of treatment routes that can taken after risk assessments are performed.

1. Avoiding the Risk- Don’t proceed with the activities that are likely to cause the risk
2. Reduce the likelihood of occurrence by implementing audits/compliance programs, formal reviews, inspection controls, etc.
3. Reduce the consequences by planning ways to continue business and reduce interdependence of activities
4. Transfer risk by using insurance, partnerships, and joint ventures
5. Accept that the risk can not be elimited or reduced and decide at what level this risk can be accepted as residual risk.

Risk reviews are to be reviewed triggered whenever there ar changes in the IT infrastructure or environment.

Across the States Bank will utilize a risk dashboard to provide a overal perspective on vulnerabilities and to prioritize the risks that need attention.

RATIONAL & JUSTIFICATION

Explain your rationale for the policy providing historical, social, professional, and legal viewpoints.

Explain how a policy decision could affect human value. Does yours? Will a one-size-fits-all policy work? Provide your justification considering the Christian worldview.

Unfortunately there is no such thing as a one-size fits all policy there for Across the State Bank's policy needs to be catered to the specific needs and assets of the organization and industry. This policy provides the basic steps for each department to have a solid foundation in determine asset identification, organization and perform risk assessments that will value the security of the information they are responsible for. From a Christian perspective it is imperative that each informational asset/data that is being managed is treated with CIA values as it can hold senstive information of real people behind the screen such as employers, consumers, leadership, etc.

The policy was developed in reflection of recent cyber incidents involving numerous financial institutions such as the event of the central bank of Bangladesh where vulnerabilities in the sofware, SWIFT, were exploited to steal over $1 billion. Proper management requires the insight of multiple professionals in the cyberspace, legal practice and information technology industry to help prevent these occurances or at least mitigate the risk and prepare organizations to be continuous.

REFERENCES

Schou, C., Hernandez, S. (2015). Information assurance handbook: Effective computer security and risk management strategies. McGraw Hill LLC.

The Global Cyber Threat to Financial Systems – IMF F&D. (2021, March 1) . https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm