Joseph Mendez
Qxo307
IS 6383-002

R&H Block Security Plan

An important topic for any institution, financial or otherwise, to implement and adhere to is security. As technology advances, these institutions must look beyond simply physical security and into cyber security as well. To assist with proper implementation for financial institutions, the IRS has a set of criteria and rules that must be abided to safeguarding taxpayer data. Aptly named Safeguarding Taxpayer Data, a checklist version of the criteria can be read here. A recent audit has revealed that R&H Block does not meet any of the requirements specified in the document. As such, an institution-wide policy framework should be put in place. This framework will serve to promote policies, standards, and controls that will not only serve to make the institution IRC compliant, but bolster the security for both our customer's data as well our network and systems.

This security plan will present various policy frameworks R&H Block may adopt to gain compliance to Safeguarding Taxpayer Data. The implementation of these frameworks will not only serve for compliance but will also make the implementation of policies and standards easier later down the line. In conjunction with these frameworks, this report will also list a series of state and federal laws that R&H Block must adhere by for IRS compliance. Afterwards, this document will list several example policies, standards, and controls that must be followed to comply with Safeguarding Taxpayer Data.

A hyperlink to each will be included for readers who want more information on the discussed topic. A short blurb as to the importance of the listed policies will also be included. Note that these examples are only and do not include all necessary policies, standards, and controls as the focus of this plan is only the user, workstation, and LAN domains. These will be developed later along with the full development of Safeguarding Taxpayer Data compliant policies.

The security plan will end with a section detailing a general plan for the implementation of the policies. The implementation plan will be later customized to each policy once these are decided upon by R&H Block Management. This general plan will be constructed following the SETA training model. Afterwards will be a brief notice pertaining to possible enforcement clauses if one of these policies is broken.

Policy Framework(s)

- NIST Cybersecurity Framework
- Sender Policy Framework
- Small Business Information Security – The Fundamentals
- Policy Framework for Effective Financial Regulation
- ISO 27001
- PCI DDS
- Control Objectives for Information Related Technology (COBIT)
- Risk Management Framework

State and Federal Laws and Regulations

- Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns
- Practice Before the IRS and Power of Attorney

- Data Breach Response: A Guide for Businesses
- Banking Regulation 2020 | USA
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley (SOX) Act of 2002
- Safeguard Rules
- Tax Information Security Guidelines for Federal, State, and Local Agencies
- US Code 6103 – Confidentiality and Disclosure of Returns and Return Information

Policies, Standards, and Controls

User Domain

Policies

- Acceptable Use Policy (AUP)
  - This policy mainly serves as the main set rules that employees and others must know when it comes to using our network. Its standards mainly cover what things should and should not be done when accessing an institution's network. These are typically signed when an employee first joins the institution. In our case, the AUP is particularly important for the organization as misuse of the network could potentially open an attack vector and put our customer's tax information and data at risk.
- Information Security Policy
  - Despite listing numerous policies covering different topics, an information security policy is one that serves as an overall approach towards security.

The Information Security Policy serves to cover and address the “CIA” triangle in cybersecurity: confidentiality, integrity, and availability. The policy is given to employees to sign as to make sure they are aware of all the standards the institution has.

- Email/Communication Policy
    - One of the most exploited vectors in institutions is email. Mainly due to human error, attackers can exploit email recipients into giving out personal or corporate data. Standards to avoid this, as well as diminishing the chances of successful email attacks, are covered in email/communication policies. Some of these include only using work email for work-related purposes and email retention standards. Seeing as preventing phishing attacks and proper email encryption is covered in the IRS Securing Taxpayer Data document, this policy should be one that is implemented.
- Clean Desk Policy
    - Aptly named, this policy’s main function is to promote a clean desk workspace for employees. While it may come off as a policy for something obvious, making sure desks are clean at the end of the workday will serve to promote physical security. Making sure employees clean their desks assures that no confidential or sensitive data remains unsecured. These could range from documents with taxpayer information to USB’s with financial data. This policy also promotes proper password management, as keeping passwords written on sticky notes is covered.

Standards

The following standards come from or are adapted from the SANS Acceptable Use Policy and the University of Chicago's Access Control Policy.

- Access to the internet from R&H Block hardware/software must only be for business use.
- Employees must report any theft, loss, or unauthorized disclosure of R&H Block information.
- Employees must also report any suspicious activity to appropriate personnel.
- Proper passwords standards must be met.
- Extreme caution when opening attachments in e-mails from unknown senders.
- Access will be monitored when account is in use.
- Multiple failed log-in attempts will cause the account to be locked.
- Users should not use personal USBs or removable devices on work devices.
- Sensitive data must be stored on devices lacking access to the internet.
- Sensitive emails should be encrypted.

Controls

Listed controls come from or are adapted from the SANS Acceptable Use Policy and both the State of Control's Control 7 and Control 15.

- Employee monitoring software
- Virtual Private Networks (VPN)
- Email monitoring software
- Access Rights Management software

- Email encryption software

Workstation Domain

Policies

- Remote Access Policy (RAP)
  - A rising trend in many businesses is the implementation of remote work for certain employees. This would allow these employees to access the network and any data stored in company servers from outside the workspace. This, however, potentially opens a vector from which hackers to attack. An AUP presents standards that help protect the network and data from threats coming from the remote domain. The policy also serves as a physical one as it also covers keeping unattended devices secure and having privacy screen protectors installed.
- Incident Response Policy (IR)
  - This policy sets out to establish a plan for institutions to follow whenever an incident is reported. Proper standards will help the institution deal with incidents as well as not hurting their brand image due to unfavorable outcomes. Proper incident response standards will include steps towards incident reporting and response; something that is necessary for IRS's Safeguarding Taxpayer Data document. This policy does not exactly work on its own as it part of a chain of policies with two others. Those will be discussed further in the list.
- Disaster Recovery Policy

  - As the second policy in the incident/disaster policy trio, the disaster recovery policy serves as the base for the disaster recovery plan. These serve to plan how a business will recover from a disaster. Its scope is not limited to a cyber-attack or server failure, disaster recovery plans also serve to allow businesses to recover from damages done in natural disasters. In the case of R&H Block, the institution should set up a DR policy and plan to be able to recover lost data and comply with Securing Taxpayer Data.

- Business Continuity Plan
  - The final part of the incident/disaster policy trio is the business continuity plan. This plan serves to put in place policies and controls that allow a business to continue to function even after a disaster or major incident. The importance of this policy is supported by its mention in Safeguarding Taxpayer Data. It achieves this by setting standards in place to mitigate the impact the institution faces. Without its implementation, institutions will have to deal with incidents on two fronts: one where they focus on recovering lost data and another in which they try to keep their business afloat.

Standards

The following standards come from or are adapted from the University of Missouri System's Workstation Management Standard.

- All Windows workstations are required to be managed by R&H Block's Active Directory system.
- All systems must be joined to the domain.
- Any antivirus software in use must be regularly updated.

- Serial number and owner information for all R&H Block systems must be kept in inventory logs by IT management.
- The Administrator account must be renamed.
- The Guest account must be disabled.
- All workstations, remote or otherwise, must be physically secured.
- Server/IT equipment rooms should be protected against physical disasters. These include but are not limited to fires, floods, or earthquakes.

Controls

Listed controls come from or are adapted from Ultimate IT Security's Top 12 Workstation Security Controls.

- Securing BIOS
- Control local accounts
- Unattended workstation controls
- Unattended workstation security controls
- Encryption
- Enable Auditing
- Anti-Malware
- Regular patching of systems
- Track new or irregular programs
- IE security configurations
- Secure settings for apps
- Proper certificate authorities

Joseph Mendez
Qxo307
IS 6383-002

LAN Domain

Policies

- Configuration Management Policy
  - The configuration management policy serves to establish standards for institutions to properly configure their assets. This policy is imperative towards the security of taxpayer data as improper configuration could lead to vulnerable systems.
- Access Control Policy (ACP)
  - The ACP is a set of rules and policies that governs over how access works as well as who has access to what. These will be managed via certain mechanisms such as access control lists and network access controls. These set of rules are essential in securing taxpayer data from unauthorized individuals and mitigating data theft.
- IT Physical Security Policy
  - While many policies exist to protect the LAN domain, the physical network access policy serves to add a tangible layer of security for an institution's networks. Some of the standards that come with this include only designated employees being able to access equipment or server rooms. Proper physical and digital security policies and measures serve to assist with protecting both data and hardware.

Joseph Mendez
Qxo307
IS 6383-002

Standards

The following standards come from or are adapted from the University of Tulsa's sample LAN Domain Network Security Best Practices and Tech Republic's IT Physical Security Policy.

- All equipment to be used must be authorized and configured with the network in mind.
- Server and data rooms must be protected with adequate security such as with guards, ID cards, etc.
- Server/IT equipment rooms should not double as neither storage nor office spaces.
- Equipment must be regularly counted and audited.
- Network equipment administration and configuration is only allowed from authorized personnel.
- Default firewall settings must deny all traffic. Only needed ports and protocols will be enabled.
- Firewall software should remain up to date.
- Logs should be regularly reviewed.
- Rules should alert administrators of both attempted and successful attacks.
- Important customer data should only be transmitted via secured VPN connections.

Controls

Listed controls come from or are adapted from the University of Tulsa's sample LAN Domain Network Security Best Practices.

- Firewalls

- Anti-Virus
- Virtual Private Networks (VPN)
- Physical securing of hardware
- Intrusion Detection and Prevention Systems
- Vulnerability Management Systems
- Network Access Controls
- Access Control/User Authentication
- Input Validation
- Encryption

Procedures and Enforcement

As with any new process or policy, proper implementation policies and training are necessary for employee awareness and compliance. Thankfully, a framework for proper training can be found in the SETA model. SETA stands for Security Education, Training, and Awareness. Each section of the SETA model is discussed in chris123205's What is a SETA program blog. The security education section deals with educating members as to how the organization prepares and reacts to situations. From here, the training section deals with providing training sessions for employees. These sessions serve to make them aware of how to properly deal with and respond to various situations. This is achieved by providing knowledge of threat detection. Leading into the final section of the model, awareness aims to increase security awareness in the employees. The official toolkit can be found on CDSE's Security Education and Training Awareness (SETA) Toolkit page.

In terms of applying this schema to R&H Block, we should hold a training session for each policy that is to be implemented. These will serve to introduce the employees to the policies as well as the impact these will have on the institution. This will be done by explaining the policy and its technicalities. Each of these sessions will end with a Question and Answer session as to iron out the employees' understanding of the policies. The sessions will either in-person or virtual/remote, depending on the employees attending.

Policies will then go into effect a week after their training session is held. During this time, all hardware must be connected to the network to have the necessary software downloaded onto it. Hardware that is required to not be connected will be updated personally by authorized IT personnel. For any remote hardware, employees will be sent a link to a VPN as a service site for them to connect to the network via a VPN. Their machines will then be updated with necessary software. Once the necessary has been downloaded, employees will be required to review and sign the policy before being able to use their hardware or access the network.

After the initial implementation, virtual training sessions will be held annually to promote employee retention of the policies. At the end of these annual meetings, employees will be asked to fill out a survey on their thoughts on the policy. These will then be used to review the policy and implement any changes. Short trainings will also be given to new employees and employees with minor policy violations.

Each policy will contain a policy enforcement clause in which actions against those who have violated the policy will be detailed. While these will vary depending on the policy, the general enforcements will be as follows:

- Verbal warning
- Forced attendance to a remedial training
- Relinquishment of certain user privileges
- Relinquishment of hardware and software licenses for remote work
- Termination from R&H Block
- Legal action based on violation or damages done