Elizaveta Vos

Week 3 Homework

**Vendor Management Policy**

**SCOPE**

This policy applies to all vendor relationships and interactions within the Hospital Authority (HA), encompassing procurement, contracting, service provision, and ongoing vendor management across all departments and operational areas.

It is applicable to all individuals involved in the vendor management process, including but not limited to procurement officers, department heads, administrators, and any personnel responsible for liaising with external vendors on behalf of the HA.

Vendors must be evaluated prior to the start of any service and thereafter on an annual basis. High risk findings must be followed up to verify remediation. A vendor risk assessment must be performed on vendors with physical or logical access to confidential information or that are considered critical vendors.

**PURPOSE**

The purpose of the HA Vendor Management Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risk to HA, its business partners, patients, and its stakeholders from any of its vendors.

This policy establishes the framework for effectively managing vendor relationships across all operational areas within the HA. The engagement of vendors is fundamental to the seamless functioning of various departments and services within the hospital. This policy aims to ensure that vendor access and interactions with hospital resources are conducted in a manner that aligns with ethical, responsible, and legally compliant practices.

The policy's applicability spans across various administrative divisions and departments within the HA. It is designed to ensure consistent adherence to security protocols and best practices, regardless of the technological environment or ownership status of the devices utilized.

**REQUIREMENTS**

In making acceptable use of resources vendors covered by this policy shall:

1. Authorized Use: Vendors must utilize hospital resources solely for purposes explicitly authorized by the HA, specifically for fulfilling contractual obligations and supporting hospital operations.
2. Protection of Credentials: Vendors are required to safeguard their assigned credentials, including User IDs and authentication mechanisms, from unauthorized access or misuse. Vendors are accountable for all activities performed under their respective credentials.
3. Access Control: Vendors shall access only information and resources for which explicit authorization has been granted by the HA or that are publicly available for vendor use.
4. Data Protection: Vendors must adhere strictly to data security policies and relevant laws when handling electronic and hardcopy data classified as High-Risk or Moderate-Risk (confidential) during their interactions with hospital systems.
5. Software Compliance: Vendors are obligated to use only legally obtained versions of software licensed by the HA, in strict accordance with vendor license agreements and contractual obligations.
6. Resource Consideration: Vendors are expected to use hospital resources judiciously, avoiding actions that monopolize resources or degrade services for other hospital staff or departments.
7. Limited Personal Use: Vendors must restrict personal use of hospital resources to minimal and occasional activities consistent with applicable laws and HA policy, ensuring that personal activities do not interfere with contractual obligations or hospital operations.
8. Content Relevance: Vendors are responsible for ensuring that all communications and materials shared within the hospital's systems and platforms are relevant to contractual obligations and hospital-related matters.
9. Confidential Data Handling: Vendors are required to store confidential data obtained during their interactions with hospital systems in approved secure locations and transmit such data only through authorized secure mechanisms designated by the HA.
10. BYOD Compliance: Vendors utilizing Bring Your Own Device (BYOD) methods must adhere strictly to approved methods designated by the HA for accessing and managing hospital systems and data.
11. Security Incident Reporting: Vendors must promptly report any identified or suspected security incidents to the appropriate authorities within the HA, following established incident reporting procedures and protocols.

In making acceptable use of resources, vendors covered by this policy shall not:

1. Unauthorized Access: Vendors must refrain from attempting to access or use another individual's system, files, or data within the hospital's network without proper authorization from the HA.
2. Password Sharing: Vendors are prohibited from disclosing their assigned passwords or authentication means to any unauthorized individuals, ensuring the integrity and security of their access credentials.
3. Security Measures Circumvention: Vendors shall not attempt to bypass or undermine any system or network security measures implemented by the HA, respecting the integrity and confidentiality of hospital systems and data.
4. Malicious Activities: Vendors must not engage in any activities intended to harm hospital systems or compromise the integrity of information, including but not limited to creating or spreading malware within hospital networks.
5. Copyright Infringement: Vendors are strictly prohibited from making or using illegal copies of copyrighted software or transmitting such copies over hospital networks without proper authorization or licensing.
6. Misuse of Communication Tools: Vendors shall not misuse email, social networking platforms, or messaging services for unlawful purposes or to harass others, maintaining professional conduct in all communications.
7. Commercial Use: Vendors must not utilize hospital systems or networks for commercial purposes without explicit authorization from the HA, respecting the intended use of hospital resources for patient care and operational activities.
8. Unauthorized Representation: Vendors are prohibited from making unauthorized use of HA trademarks or logos or falsely claiming to represent the organization in any capacity.
9. Violation of Laws and Policies: Vendors must adhere to all applicable laws, regulations, and HA policies governing IT resource usage, ensuring compliance with legal and ethical standards.
10. Unsolicited Communications: Vendors shall refrain from sending commercial or personal advertisements or solicitations unrelated to hospital business via hospital communication channels, respecting the professional environment and focus on patient care.
11. Insecure Transmission of Data: Vendors must ensure secure transmission of confidential information over the internet, utilizing appropriate security measures to safeguard patient data from unauthorized access or interception.
12. Unauthorized Data Modification: Vendors must not modify hospital information resources or technology without proper authorization from the HA, respecting the integrity and reliability of hospital systems and data.
13. Insecure Data Storage: Vendors shall not store confidential data obtained during their interactions with hospital systems on local drives, external media, or unauthorized locations, ensuring data security and compliance with hospital policies and regulations.

**MANAGEMENT**

1. The HA's IT security team will conduct regular monitoring and auditing of vendor access and interactions within the hospital system to ensure adherence to this policy.
2. Periodic access reviews will be conducted to analyze access logs, identify any unauthorized activities, and verify that access privileges granted to vendors are appropriate and current.
3. Any deviations, anomalies, or security incidents detected will be promptly investigated and addressed following the HA's incident response procedures, with appropriate actions taken to mitigate risks and ensure compliance.
4. Non-compliance with this policy may lead to disciplinary measures, including the restriction or termination of network privileges for vendors, in accordance with established HA policies and procedures.
5. The HA's IT department holds responsibility for maintaining and enforcing this policy. They are tasked with regularly reviewing and updating the policy to reflect changes in technology, regulations, and security standards. Furthermore, they are responsible for overseeing compliance with this policy and implementing disciplinary actions as necessary for violations.

**ENFORCEMENT**

Vendor found to have violated this policy may face disciplinary measures, ranging from warnings to termination of contract, as well as potential civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may face sanctions, including the revocation of access rights, termination of contract(s), and potential civil or criminal penalties.

**WAIVERS**

Waivers from Vendor Management Policy may be sought following the HA Waivver Proces.

**REFERENCES**

* NIST SP 800-161r1 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>
* Vendor Non-Disclosure Agreement/Business Associate Agreement

Last revised April 19, 2024 Version 1.0