University Health Network
Policy & Procedure Manual
Administrative – Vendor & Related Party Access

Policy

University Health Network (UHN) secures and protects the information assets it owns. UHN provides information technology (IT) resources to meet the business and strategic needs of the organization. UHN grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Vendors must satisfy the conditions stipulated in this policy to connect to UHN network infrastructure. Only those vendors that meet the requirements specified in this policy or are granted an exception by the Information Security Department are approved to use UHN IT resources.

All vendors, contractors, or consultants, including all personnel affiliated with third parties that provide a service to UHN, must adhere to this policy. Services may include but are not limited to:

- software or hardware support
- development or testing
- assessments or audits
- data mining or reporting

The Information Security Department must approve temporary exceptions to this policy in advance.

Conditions

All external parties such as vendors, contractors, consultants must:

- Abide by all UHN policies, including but not limited to:

  a. Appropriate Use of Technology policy 1.40.012
  b. Code of Conduct (on UHN Intranet home page)
  c. Conflict of Interest policy 2.50.002
  d. Privacy policy 1.40.007
  e. Press Releases policy 1.50.003

- Complete the UHN Vendor Access Agreement.

- Have at least one contact at UHN for the purpose of the engagement.

- Provide a list of all individuals who will access UHN IT resources. The list must be updated within 24 hours of any changes.

- Identify all individuals who are not directly employed by the requesting party.

- Upon a departure of an employee, ensure that all UHN assets are collected from that employee and ensure that access and credentials are updated appropriately.

- Any security incidents directly or indirectly related to the service provided to UHN must be notified to Information Security officer or Privacy officer within 24 hours.

- Follow UHN change management processes.

- Agree on a regular schedule during which UHN IT resources are accessed. Any exceptions must be approved in writing by the appropriate UHN staff in advance.

- Return or destroy all materials, information, assets, access cards, and any other UHN resources within 48 hours of contract termination.

- Ensure that any systems connecting or using IT resources are secure and stable. Anti-virus, encryption methods, firewalls, application patches and other safeguards must be up-to-date and effective.

- State that necessary insurance provisions have been arranged to cover any potential damages to UHN including any the activities of outsourced entities.

Vendor activities on any UHN site or location may be supervised by a UHN employee or monitored via any other means.

Prior to requesting access, the Vendor Access Agreement form has to be completed and signed off. The UHN sponsor or project manager must ensure that this document is kept up to date.

All access granted to a vendor must follow the least-privileges principle. Access credentials such as usernames and passwords must be communicated securely and directly to the individual intended. Accounts must only grant access to specific systems or applications for support purposes only. Due diligence must be taken to ensure that the activity is audited, where technically feasible.

Usernames and passwords granted to a vendor must follow guidelines for the expiry period and complexity.

UHN reserves the right to audit any activity or suspend access for operational purposes.

Breach of Policy

Failure to adhere to this policy may result in the suspension or loss of access privileges as well as other measures, up to and including termination of the contract.