HTN Policy for Vendor & Third-Party Access

HELP THE NEEDY
CHARITABLE TRUST

HTN POLICY for Vendor & Third Party Access

Contents

1. Purpose

The HTN Vendor/Third Party Access Policy informs HTN management, business owners, IT project teams and support staff of the HTN requirements for vendor access to HTN Information Systems.
The policy defines vendor responsibilities for the protection of HTN information and information systems.

2. Scope

The HTN Vendor Access Policy applies to all individuals and/or parties that are responsible for the installation of new HTN Information System assets, and the operations and maintenance of existing HTN Information Systems, and who do or may allow vendor access for support, maintenance, monitoring and/or troubleshooting purposes.

3. Policy

a) Vendor access to HTN Information Resources is granted solely for the work contracted and for no other purposes.

b) Vendors must comply with all applicable HTN policies, practice standards and agreements, including, but not limited to:

- OH&S Policies
- Change Management Policies
- Privacy Policies
- Security Policies
- Auditing Policies
- Software Licensing Policies
- HTN Code of Conduct

c) Vendor agreements and contracts must specify:

- The HTN information the vendor should have access to. If, at the time of contract negations this is unknown or ambiguous, mention of this should be made in the agreement.
- How HTN information is to be protected by the vendor. A copy of the Vendor's Security and Privacy Policy should be made available to HTN where appropriate.
- Acceptable methods for the return, destruction or disposal of HTN information in the vendor's possession at the end of the contract.
- Agreement that the Vendor must only use HTN information and Information Systems for the purpose of the business agreement.
- Any other HTN information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

d) Where applicable, HTN will provide a technical point of contact for the vendor. The point of contact will work with the vendor to ensure the vendor is in compliance with HTN policies.

e) Where applicable, the business owner will provide the vendor with a point of contact from within the relevant School, Section or Division. The internal point of contact is responsible for liaising with HTN for all relevant Change Management processes.

f) Before the commencement of the agreement the appropriate implementation of HTN change management processes will be determined by HTN in consultation with the Vendor and the HTN business owner. This will include such things as the definition of standard changes, level and type of communications around changes, and responsibilities around technical vulnerability management and security incident reporting.

g) At the commencement of the agreement, Standard Changes, as defined in the context of the HTN change management system, must be clearly identified and agreed upon by the Business Owner, The Vendor and DIT.

1 All work and changes that are identified as impacting on other HTN systems must be entered into the HTN Change Management System by the HTN point of contact or, where applicable, the Business Owner point of contact. Activities include, but are not limited to, such events as software/operating system updates/patches, password changes, project milestones, changes to deliverables, and commencement and completion times, wherever possible.

h) Vendors work activities on HTN systems may be monitored and logged for comparison to Change Management System records.

i) Before the commencement of the agreement, methods for:

- The monitoring and review of service performance,
- logging activities,
- submission of vendor reports and,
- roles and responsibilities regarding problem management

will be determined by HTN in consultation with the Vendor and the HTN business owner.

j) Each vendor must provide HTN with a list of all employee names working on the contract. The list must be updated and provided to HTN within 24 hours of staff changes, wherever possible.

k) Vendor access must be uniquely identifiable and password management must comply with the HTN Password Policy and the HTN Remote Access Policy.

l) If appropriate, regular work hours and duties will be defined in the contract. Work outside of defined timeframes must be approved by the appropriate HTN business owners

m) All vendor maintenance equipment on the HTN network that connects to the internet via any means, and all vendor accounts, will remain disabled except when in use for authorized maintenance.

n) Upon departure of a vendor or vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to HTN or destroyed within 24 hours.

o) Upon termination of contract, or at the request of CSU, the vendor will return or destroy all HTN information and provide written certification of that return or destruction within 24 hours.

p) Upon termination of contract, or at the request of DIT, the vendor must surrender all HTN access cards, badges, and equipment immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized HTN management.

q) Vendors are required to comply with all regulatory and HTN auditing requirements, including the auditing of the vendor's work.

r) All software used by the vendor in providing service to HTN must be properly inventoried and licensed.

s) Each vendor granted access to any HTN Information System must sign the HTN Vendor Security, Privacy, Copyright and Confidentiality Agreement Form which stipulates that each individual:

- Has read and understands the security policies
- Understands the responsibility to comply.
- Understands the consequences of an infraction.