Third-Party Access Policy

Purpose

The Purpose of the USEK Third-Party Access Policy is to establish the rules for third-party access to USEK information systems and the computer room, third-party responsibilities, and protection of USEK information.

Scope

The USEK Third-Party Access Policy outlines the responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of the USEK personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to, software vendors, contractors, consultants, business partners and security companies.

Policy

Server Room: Third Party Policy Guidelines

1. All third-party access to the server room should be scheduled to occur during regular business hours. If this is not possible, a point person, from the IT department, will be scheduled, after hours, to accompany the third party.

2. When third parties are scheduled to have access to the server room, the Information Technology Services staff must be notified in advance of the date, time, and type of work to be performed.

3. When the third party arrives, he/she will report to the staff contact that scheduled the visit. The staff contact will escort the third party to the Information Technology Services area. At this point, the third party is to be informed that he/she will take further direction from the IT staff point person, in relation to their activity in the server room.

4. Prior to the onset of any work, the third party will describe the activities that are planned

5. The IT staff point person is responsible for explaining what measures need to be taken to protect the computer/server’s hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems, before starting their work.

6. The third party will report to and receive instructions from the IT staff point person regarding their work in the server room. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed, before leaving the area.

Information Systems: Third-Party Policy Guidelines

1. Any third-party agreements and contracts must specify:

   - The work that is to be accomplished and work hours. Also, any configuration information of any installed software, as well as virus checking of that software.
   - The minimum security requirements that the third party must meet (i.e., method for remote access).
   - How USEK information is to be guarded by the third party. Signing of a non-disclosure agreement is typically required.
   - Strict use of USEK's information resources for the purpose of the business agreement by the third party. Any other USEK information, acquired by the third party in the course of the contract, cannot be used for the third-party's own purposes or divulged to others.
   - Feasible methods for the destruction, disposal, or return of USEK information at the end of the contract.
   - The return of USEK property, such as a laptop, PDA, or cell phone, after the completion or termination of the agreement.

2. The third party must comply with all applicable USEK standards, agreements, practices and policies, including, but not limited to:

   - Acceptable use policies.
   - Software licensing policies.
   - Safety policies.
   - Auditing policies.
   - Security policies.
   - Non-disclosure policies.
   - Privacy policies.

3. USEK will provide an IT point of contact for the third party, whether it is one person from the IT department or an interdepartmental team. This point of contact will liaise with the third party, to ensure they are in compliance with these policies.

4. The third party will provide USEK with a list of all additional third parties working on the contract. The list must be updated and provided to USEK within 24 hrs of any staff changes.

5. Third party access to systems must be uniquely identifiable, authenticated and password management must comply with the USEK Password Policy. Managing connectivity with partner networks can be handled in different ways, depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).

6. Any third party computer/laptop/PDA/tablet PC that is connected to the USEK systems, must have up-to-date virus protection and patches. The third party will be held accountable for any damage that transpires to USEK, in the event that an incident occurs.

7. If applicable, each third party on-site employee must acquire an USEK ID badge that must be displayed at all times while on the premises. The badge must be returned to USEK upon termination or completion of the contract.

8. Each third-party employee that has access to USEK sensitive information should be cleared to handle that information.

9. If applicable, an explanation of how USEK information will be handled and protected at the third party's facility/site must be addressed.

10. Third-party employees must report all security incidences to the appropriate USEK personnel.

11. If third-party management is involved in USEK security incident management, the responsibilities and details must be specified in the contract.

12. The third party must follow all applicable change control procedures and processes.

13. All software used by the third party, in providing service to USEK must be properly inventoried and licensed.

14. All third-party employees are required to comply with all applicable auditing regulations and USEK auditing requirements, including the auditing of the third-party's work.

15. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the appropriate USEK management.

16. All third-party maintenance equipment on the USEK network that connects to the outside world via telephone lines, leased line or the network will remain disabled except when in use for authorized maintenance.

17. The third party's major accomplishments must be documented and available to USEK management upon request. Documentation should include, but is not limited to events such as:

    - Personnel changes.

- Password changes.
- Project milestones.
- Deliverables.
- Arrival and departure times.

18. USEK will perform an impact analysis of other business-critical functions, once work has begun by the third party.

19. USEK will monitor system and network log files 3 times per week/day.

20. USEK will eliminate third-party physical access to facilities after the contract has been completed or terminated. The following steps must be performed:

    - Remove third party authentication and all means of access to systems.
    - If needed, make sure that incoming e-mail is re-routed to an appropriate person.
    - Archive any third-party software configuration, and transfer ownership to designated internal staff.
    - Get a written statement from the third party that any software created and/or installed by the third-party is free of viruses and any other malicious code.

Enforcement

Any employee or third party who is found to have violated this policy may be subject to disciplinary action, up to and including termination of contract.

Third-Party User Agreement

I have read and understand the Third-Party Access Policy. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to applicable law or USEK policy.

Name: ____

Signature: ____

Date: ____