City of Fredericksburg

Third Party Access Policy

Purpose

The purpose of the City of Fredericksburg Third Party Access Policy is to establish the rules for Third Party access to City of Fredericksburg (herein after "City") information systems, Third Party responsibilities, and protection of City information.

Scope

This Third Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to City information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of City 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 Rooms

The Third Party agrees to follow the City **Server Room Access Policy**.

Third Party Policy Guidelines

1. The Third Party agrees to / that:
    - All work shall be scheduled with and pre-approved by the City's Information Technology Department (herin after " IT"). Also, all configuration information of any installed software as well as virus checking of that software shall be made available to IT.
    - The Third Party shall have access only to City information that has been pre-approved by IT.
    - Meet the following minimum security requirements (i.e. method for remote access).
        - Any remote support connection must be encrypted with a minimum of AES128 bit encryption.

- Any remote support connection must have an inactivity timeout with a maximum of 15 minutes.
- Any remote support connection must be configured to allow the City of Fredericksburg to monitor the remote session.
- Remote support access shall follow the minimum amount of rights to complete their responsibilities.
- Remote support access must be configured in a way that the City can disconnect at any time.
- Remote support access from a Third Party must have an up to date and operational virus /malware scanner.
- Remote support access from a Third Party must also be secured by either a software based firewall installed on the computer or a hardware based solution. It must be up to date and operational.
- Any special considerations must be approved by IT.

- City information shall be guarded by the Third Party. Signing of a **Non-Disclosure Agreement** is required.
  - This includes the disclosure of confidential information to anyone, including City staff (ex. Passwords).
- The Third Party agrees to use City information only for the purpose of performing work for the City. Any City information acquired by the Third Party shall not be used for the Third Party's own purposes or divulged to others.
- Without the City's written permission, no one may extract, use or reuse all or any part of the database, judged quantitatively or qualitatively, in a manner that conflicts with the normal exploitation of the database in actual or potential markets. This prohibition applies whether the database is misappropriated all at once or through repeated or systematic, small takings, and whether the defendant takes the database personally or does so through agents or contractors.
- Specific prohibited acts include using all or any part of the contents of the protected database (1) in a directly competitive product or service; (2) in a product or service that directly or indirectly competes in any market which the database owner has a demonstrable interest or expectation of entering; (3) in a product or service marketed to those who would otherwise be expected to be customers for the original database; or (4) by or for multiple users within an organization who may "piggyback" additional uses or additional users not in concert with the original authorization by the owner.

2. The Third Party must comply with all applicable City 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.

(Copy of policies available upon request)

3. The City shall provide an Information Technology point of contact for the Third Party whether it is one person from the IT department or an interdepartmental team. This point of contact shall liaise with the Third Party to ensure they are in compliance with these policies.

4. The Third Party shall provide the City with a list of all additional Third Parties working on the contract. The list must be updated and provided to the City within 48 hours of any staff changes.

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

6. Any Third Party computer/laptop/tablet PC, or other device, that is connected to the City's systems must have up-to-date virus protection and patches. The Third Party shall be held accountable for any damage to the City's network and/or data should it be determined that the incident was directly related to that Third Party's access.

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

8. Upon request, each Third Party shall ensure and provide documentation that their employees that have access to City confidential information have been cleared to handle that information.

9. Upon request, an explanation of how City information shall be handled and protected at the Third Party's facility/site must be provided.

10. Third Party employees must report all security incidences to City IT personnel.

11. The Third Party must follow all applicable change control procedures and processes.

12. All software used by the Third Party in providing service to the City must be properly inventoried and licensed.

13. All Third Party employees are required to comply with all applicable auditing regulations and City auditing requirements, including the auditing of the Third Party's work.

14. Regular work hours and duties shall be defined in the contract. Work outside of defined parameters must be pre-approved in writing by IT.

15. All Third Party maintenance equipment on the City's network that connects to the outside world via any communication path shall remain disabled except when in use for authorized maintenance.

16. The Third Party's major accomplishments must be documented and available to City management within 48 hours. Documentation should include, but is not limited to events such as:

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

17. Upon departure of the Third Party from the contract for any reason, the Third Party shall ensure that all confidential information is collected and returned to the City or destroyed within 48 hours. The Third Party shall also provide written certification of that destruction within 48 hours. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the Third Party must be documented and authorized by the City IT Department.

18. The City may perform an impact analysis of other business-critical functions, once work has begun by the Third Party.

19. The City may monitor system and network log files.

20. The City shall 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, ensure that incoming e-mail is re-routed to an appropriate person.
    - Archive any Third Party software configuration, and transfer ownership to designated internal staff.
    - Obtain 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.

21. The Third Party agrees that:

- Electronic self-help shall not be used to prevent the City's use of Systems and that the City shall only be deprived of the use of Systems by order of a court of competent jurisdiction.
- The Application Software shall not contain any undisclosed restrictive code or automatic restraints that are not specifically and expressly authorized in this Agreement.
- They shall not introduce any restraints at a future date via remote access, software update or any other means without first obtaining approval from the City in writing.
- No limitation of liability or consequential damages shall apply to a breach of the aforementioned provisions.

Non-Compliance

Violations of this policy shall be treated like other allegations of wrongdoing at the City of Fredericksburg. Allegations of misconduct shall be adjudicated according to established procedures. Sanctions for inappropriate use on the City of Fredericksburg's systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of system access;
2. Determination of breach of contract;
3. Termination of contract; and/or
4. Legal action according to applicable laws and contractual agreements, including action to recover monetary damages for breach 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 action according to applicable law.

Name: _____

Signature: _____

Date: _____