Acknowledgement of Expectations of Remote Access

- Hourly (non-salaried) employees must have pre-authorization for any work done from a remote location.
- Employee must ensure that anti-virus is up to date prior to each connection to the City network.
- Employee is responsible for any costs associated with the connectivity from the personal computer to the City network.
- Employee is responsible for maintaining confidentially of the remote access usernames and passwords, including but not limited to:
    - Not sharing usernames and passwords with others.
    - Not writing usernames and passwords down.
    - Not passing usernames and passwords via email.
- The password assigned to you must be protected at the same level as the information processed on the system(s). You are responsible for any activity on your account.
- Your password is unique to your user-ID and identifies your individual system authority and privilege. It must not be shared with anyone else, even individuals working on the same project.
- Passwords shall not be included in script files for logon procedures, automatically programmed into function keys or written down.
- If you believe that the confidentiality of your password has been compromised, contact the Cybersecurity Office immediately. If your password is changed for any reason, you will be notified immediately.
- Any equipment connected to the City Network may be scanned and activity monitored to ensure the security of the City Network and Systems.
- Non-exempt employees must receive department authorization prior to using remote access.

Rules for Contractor and Volunteer Access

- City of San José (City) data, communications, software, hardware, services, and related technology resources are only for assigned uses.
- Contractor access accounts will be approved for durations of **6 months or less**, based on the needs of City Departments and approvals.
- To protect City resources and assets from unapproved access and misuse, City contractors and volunteers are responsible for all activity conducted under unique credentials and shall:
    - Not share their logins and/or passwords nor use those of others;
    - Secure City technology assets when not in active use;
    - Not install or connect any software or hardware to City resources without prior approval from the City IT Department;
    - Not store or access any City data without prior approval from a City Department Director; and
    - Return any and all City assets and data within two days of contract conclusion or termination unless otherwise approved by the City.
- City email accounts are not permitted for contract employees. If an exception is made, non-employee status must be indicated in the address.

Examples of Prohibited Activity Include, but are not Limited to, the Following:

- Use of the City of San José's computer systems for any activity without a business-related purpose, including, but not limited to, any illegal and/or discriminatory activity.
- Communicating any privileged work product, restricted data, and/or confidential information, without appropriate City approval and handling.
- Avoid any communications that violate copyright laws; intimidate or threaten others; constitute violations of any City Policy, including, but not limited to the City's Code of Ethics Policy and/or Discrimination and Harassment Policy; and/or interferes with the ability of others to conduct official City business.
- Constructing or changing an electronic message so it appears to be from someone else and/or contains false content.
- Breaching or attempting to breach City information security measures, and/or intercepting communications, data, and/or information.
- Knowingly or carelessly running any software and/or malware that may impair City operations.
- Contractors and volunteers must notify IT Cyber Security and their direct supervisor immediately once they become aware of any violation of the terms covered in this acknowledgement.