CITY OF VANCOUVER

CORPORATE POLICY

POLICY TITLE	Technology Third Party Access
CATEGORY	Administrative
POLICY NUMBER	ADMIN-040
LEGISLATION	Freedom of Information and Protection of Privacy Act (BC)
POLICY OWNER	Chief Technology Officer, Technology Services
ACCESS	Public

PURPOSE

When required, Third Party access is granted to City information and technology. This policy sets out the requirements on City staff with providing such access to contractors, vendors, suppliers, service providers or any other Third Party. This policy replaces the *Letter of Understanding for Non Employees (04-0500-11/00050)*.

SCOPE

This policy applies to all instances of access to the City's technology by a Third Party.

DEFINITIONS

"**access**" means access in any format and by any means to the City's Technology, including by on-site visual access, remote access, or by access via an external storage device.

"**City Technology**" means any of the City's information or data in any format, including that which is stored on any computers, networks, databases, operating systems, or other software, or cloud-based systems or servers, and including all proprietary and intellectual property related to such information, data, and software which is owned or controlled by the City or for which the City is responsible under FIPPA.

"**FIPPA**" means the Freedom of Information and Protection of Privacy Act (British Columbia), as amended or replaced from time to time.

"**Fulfillment Date**" means the date the service in enabled for use.

"**Third Party**" means any corporate or individual entity including without limitation any corporation, partnership, individual, society, governmental agency, or other legal entity which is external to the City and the City's employees.

POLICY STATEMENTS

1. **General – Access Prohibited**
   No City staff are permitted to provide Third Party access to the City's Technology unless expressly permitted by this Policy.

2. **Limits to Access**

City staff requesting access to the City's technology on behalf of a Third Party can only do so after verifying, confirming and recording in their written records that one or more of the following conditions is in place:

(a) The Third Party has a written services contract in place with the City which was entered into in accordance with the City's Procurement Policy and contains a confidentiality clause and the City staff has received written acknowledgement from the Third Party that the access is being provided pursuant to that contract and the confidentiality obligations in same.

(b) The Third Party has entered into a Non-Disclosure Agreement or Confidentiality Agreement with the City and the City staff member has confirmed that such agreement was reviewed and approved by Legal Services and has received a written acknowledgement from the Third Party that access is being provided pursuant to that NDA or CA and the Third Party's obligations under same.

(c) The Third Party has entered into an information-sharing or similar agreement with the City and such agreement has been approved by the applicable General Manager and City Solicitor pursuant to the Non-Standard Agreements Policy (or by Council) and the City staff member has received a written acknowledgement that the access is being provided pursuant to such agreement and will be bound by its obligations under same with respect to such access.

(d) There is no existing agreement of the type described in (a) and (b) above, but the Access has been approved in writing by the City Solicitor and Chief Technology Officer, and the City staff has complied with all conditions set out by the City Solicitor and Chief Technology Officer in relation to the access.

3. **Providing Access Once Authorized**

Provided Section 2 above has been fully complied with, City staff may then make a request through ServiceNow. The business unit of the staff requesting access will cover any costs associated with providing access (e.g. VPN.)

Third Party accounts are to be set with an expiry date of no more than 1 year from the Fulfillment Date. Account extensions can be requested 60 days prior to the account expiry date via a ServiceNow Account Extension request.

Users must use Multi-Factor Authentication (MFA) for City computing resources that require MFA and for remote access to the City network. If users do not use MFA, they will not be able to access these resources.

4. **Additional Policies and Procedures**
City staff are responsible (to the City as their employer, not to the Third Party which will always have under the applicable agreement or contract a legal duty to the City to comply) to make sure the Third Party, inclusive of maintenance and support personnel, are aware and comply with the security measures put in place by the City, including procedures directed towards the collection, use and disclosure of personal and confidential information under FIPPA.

This rule is designed to provide an extra layer of protection for the City in helping to ensure that all access by Third Parties is compliant with the City's Enterprise Data Policy, the City's Privacy Policy and FIPPA.

5. **Terminating access**
The City reserves the right to terminate Third Party access at any time, for any reason, without notice. City staff must report any non-compliance of which they become aware to the Chief Technology Officer immediately who in turn must consult with the City Solicitor as to the City's legal and contractual rights to terminate access by the applicable Third Party.

6. **Supervised Access Preferred**
When possible, City staff should endeavour to provide access through screen sharing tools (e.g. Webex) or similar methods. These methods of access are recommended as they greatly enhance the level of security provided to the City's technology and may promote knowledge transfer to City staff.

7. **Unsupervised Access**
When necessary, a Third Party may be provided with an Active Directory ID (user ID and password) and a City approved connection method (e.g. VPN) for unsupervised, ongoing access. In these circumstances, City staff must take reasonable steps, in consultation with Technology Services, to structure the access on the basis of least access required to enable completion of the City's obligations under the applicable agreement. This includes access to as little information as is necessary, access for as short a duration as is reasonably possible, and in some cases may require additional security checks as per the City's Positions of Trust Policy.

8. **Confidentiality**
City staff are to be vigilant and monitor the Third Party's access to the City's technology to the best of their ability so as to be alert to possible breaches of the Third Party's obligations:

   (a) not to disclose confidential, proprietary, or personal information;

   (b) to maintain the security of the City's facilities by keeping IDs, passwords, dial-in telephone numbers, internal domain names, IP addresses and any other details of the City's security systems confidential; and

(c) not to use the access for any purpose outside of the purposes expressly permitted under the applicable agreement or contract under which the City granted the access in the first place, including without limitation, selling, trading or financially benefitting from the access except in accordance with the agreement.

9. Security and data disposal

City staff are encouraged to consult with Technology Services to ensure that the Third Party has appropriate security measures in place on devices accessing the City's network, including current antivirus software, updates and security patches. For security reasons, the Third Party is prohibited from forwarding City records, data and work files to non-City email addresses.

Data generated by a Third Party while doing City work belongs to the City unless stipulated otherwise by a contractual agreement.

Before the end of a contract or agreement, City staff must ensure that the Third Party has complied with its obligations to:

(a) ensure all information and data has been securely transferred to the City;

(b) undertake secure data disposal measures to ensure all City data is removed from non- City devices;

(c) provide written confirmation of data disposal; and

(d) use the Service Now Employee Departure Form to ensure the account is off-boarded.

10. Exemptions

The City's Chief Technology Officer or a Director with express written authority delegated to them by the City's Chief Technology Officer (in consultation with the City Solicitor) may grant standing or single instance exemption to this policy where a valid business reason exists. Exemptions will be tracked and reviewed annually.

11. Violations

Any violation of this policy may result in disciplinary action up to and including termination.

12. References

This policy must be read and applied in conjunction with the City's following related corporate policies: Corporate Procurement Policy (ADMIN-008), Technology Acceptable Use (ADMIN-35), Cybersecurity (ADMIN-36), Network Connectivity (ADMIN-37), Enterprise Data (ADMIN-38) and Technology Lifecycle (ADMIN-39.)

APPROVAL AND REVIEW HISTORY:

Version 1 approved by:	Director, Enterprise Technology	11/5/2020
	Chief Technology Officer	12/14/2020
Version 2 approved by:	Director, Enterprise Technology	11/14/2022
	Chief Technology Officer	11/14/2022

Next review date 11/14/2024