**Administrative Regulations**
**Office of the Mayor**
**Title:** ELECTRONIC ACCESS BY THIRD PARTY
**A.R. Number:** 2.11 **Effective Date:** 2/1/2009 **Page:** 1 of 5
**Supersedes:** N/A **A.R.:** N/A **DATED:** N/A

## I. PURPOSE

This policy outlines the procedures that third party organizations must follow when connecting to the City of Richmond (COR) networks for the purpose of transacting business related to the COR.

## II. SCOPE

Electronic connections between third parties that require access to non-public COR resources fall under this policy, regardless of whether a telecommunications circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for the COR or to the Public Switched Telephone Network does NOT fall under this policy.

## III. PROCEDURE

A. Security Review

All new network connectivity will go through a security review with the Department of Information Technology (DIT). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

B. Third Party Connection Agreement

All new connection requests between third parties and the COR require that the third party and the COR representatives agree to and sign a *Memorandum of Agreement* (sample copy attached). This agreement must be signed by the COR user department director as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the DIT Network group.

C. Business Case

All production network connections must be accompanied by a valid business justification, in writing, that is approved by the DIT Network Manager and the DIT Security Manager. Typically this function is handled as part of the *Memorandum of Agreement*.

D. Point of Contact

The third party organization must designate a person to be the Point of Contact (POC) for the network connection. The POC acts on behalf of the third party organization, and is responsible for those portions of this policy and the *Memorandum of Agreement* that pertain to it. In the event that the POC changes the DIT Network Manager must be informed promptly.

E. Establishing Connectivity

Sponsoring departments in the COR that wish to establish connectivity to a third party are to file a new site request with the DIT Network Manager. The DIT Network Manager and DIT Security Manager will address security issues inherent in the project. The sponsoring department must provide full and complete information to the DIT Network Manager and DIT Security Manager as to the nature of the proposed access by the third party.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will the COR rely upon the third party to protect COR's network or resources.

F. Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via the DIT Change Control Notification process. The sponsoring department is responsible for notifying the DIT Network Manager and DIT Security Manager when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

G. Terminating Access

When access is no longer required, the sponsoring department in the COR must notify the DIT Network Manager responsible for that connectivity, which will then terminate the access. Termination of access may mean a modification of existing permissions up to terminating the circuit, as appropriate.

The DIT Network team must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, or are no longer being used to conduct COR business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct COR business necessitate a modification of existing permissions, or termination of connectivity, the DIT Network team will notify the DIT Security Manager, the POC, and the sponsoring department of the change prior to taking any action.

## IV. RESPONSIBILITIES

Third Party users are held responsible to use these systems according to this policy. Any Third party user found to have violated the COR's policy on access may be terminated from current and future use. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## V. DEFINITIONS

| **Terms** | **Definitions** |
|---|---|
| Circuit | For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies. |
| Employees | For this policy, employees include all individuals who use the city's electronic information systems/network e.g. but not limited to, employees, contractors, vendors, temporary agency staff, and state agencies. |
| Sponsoring department | The COR department who requested that the third party have access to the COR information through electronic methods/media. |
| Third Party | A business entity or person that is not a formal or subsidiary part of the COR. |

## VI. REGULATION UPDATE

The Department of Human Resources and the Department of Information Technology shall be responsible for modifications to this Policy.

**APPROVED:**

**MAYOR**

## *MEMORANDUM OF AGREEMENT*

*(Page 1 of 3)*

City of Richmond Department of Information Technology and Third Party User

### Summary

This Memorandum of Agreement (MOA) specifies the responsibilities of the City of Richmond (COR) Department of Information Technology (DIT) and Third Party Users (TPU) in deploying and supporting TPU computer equipment on DIT's network. The essence of the agreement is that the TPU network will be integrated into the DIT network, with DIT assuming full responsibility for the network infrastructure. The TPU will provide primary support for all PCs, servers and applications wholly owned by the TPU, with DIT available for second-level support of these systems if needed.

DIT supports an extensive citywide network comprising numerous LANs interconnected by a variety of wide-area networks (WANs). This network provides many information resources, including Internet access and a number of programs which support mandated federal and state programs or law enforcement services. Because TPU need to use many of these resources, we are in agreement that incorporating TPU network into the DIT network allows for the best use of City resources and provides TPU the most efficient access to the resources it needs.

### Automation Coordinator

TPU will designate an Automation Coordinator who will serve as the primary contact with DIT for automation and security needs. Duties include handling security issues, telecommunications inventory and requests for network and telephone services. The Automation Coordinator may be required to attend monthly Automation Coordinator meetings held by DIT.

### Security

Although TPU network will become part of a network operated by DIT, it is important to maintain security so that the data belonging to TPU and to the City is accessible only to authorized users. While such security is a normal aspect of network operation, special cooperation will be required here because the servers and other information resources will be managed by two different staffs.

Each party agrees to provide to the other documentation describing the procedures, standards and rules followed in managing systems connected to the network, and to ensure that access to network resources is limited to those users who have been properly authorized in compliance with these policies.

The TPU Automation Coordinator, with the help of DIT, will use the *System Access Privilege Request* (SAPR) application to submit requests for security authorizations to resources managed by DIT.

Each authorized user of computing resources will be provided with a unique username and password in order to access the system. Multiple users may not share these usernames. Each user must agree to sign the Statement of Responsibility form. The original Statement of Responsibility form will be filed by the department with whom the TPU is working. The Statement of Responsibility form must be made available to the City Auditor on request. There will be an automatic time-out or required re-authentication after a predetermined amount of time with no user activity. The DIT security administrator must be notified immediately of any changes in personnel status (termination, re-assignment, etc.) that affects a user's right to access information resources.

## *MEMORANDUM OF AGREEMENT*

*(Page 2 of 3)*

City of Richmond Department of Information Technology and Third Party User

### Standards

TPU agree to adhere to all DIT standards pertaining to information access, network management and PC hardware and software on network-connected PCs. These include but are not limited to:

- Hardware Standards for Personal Computers
- Software Standards for Personal Computers
- Network Responsibility Standard
- Processing Purchase Orders for Computer Hardware and Software
- Data Security Standard
- Information Service Request Standard
- Backup and Restore Standard

TPU will be allowed to use City mail and Internet services without charge, provided that TPU either adopts *City Administrative Policy 2.5* governing the use of electronic media systems or develops a similar policy that is acceptable to DIT. Failure to enforce such a policy will result in the cancellation of these services.

### Help Desk

TPU will call their staff to report all computer and network problems or issues. The TPU staff will attempt to resolve problems related to PCs or applications belonging to TPU. In the event that the problem appears to relate to COR network infrastructure or to DIT-controlled resources, the TPU Automation Coordinator or designated representative will call the DIT Help Desk to open a problem log with DIT.

### Information Service Request

If TPU need to have DIT carry out a project requiring more that eight hours of work, TPU will prepare an *Information Systems Request* (ISR) form and submit it to the appropriate Project Leader in DIT. TPU agree to participate in the Automation Plan by providing input on their projected IS project needs in a timely manner.

### Contract Support

DIT, acting as the City's agent, agrees that TPU may participate in DIT's Contractual and Franchise agreements with vendors.

### Audit

With prior notice, TPU agree to allow designated DIT and/or City Internal Audit staff (City Auditors) to visit TPU sites and, under supervision of TPU staff, to inspect the rules, policies and records pertaining to operation of TPU computer systems and network. The purpose of any inspection is to ensure TPU comply with the terms and conditions noted herein. The same condition applies to DIT. TPU may audit DIT for compliance. Each party agrees to notify the other within 30 working days on any instance of suspected or demonstrated noncompliance. Both parties agree to correct any deficiency noted by the other.

The City of Richmond assumes no liability in the case of software license copyright violations. In some instances TPU will agree to incorporate all computer systems under the Microsoft Enterprise Licensing program.

Both parties agree not to disclose any information in its possession about the other's environment to any third party not identified in this MOA.

## *MEMORANDUM OF AGREEMENT*

*(Page 3 of 3)*

City of Richmond Department of Information Technology and Third Party User

### Training

Instructor-led or video training as offered to the City by DIT will be free of charge.

### Server Systems

All backup/restore functions for TPU servers are the responsibility of TPU. The City has not included TPU in Disaster Recovery or Business Continuity Resumption Services, although TPU will be able to utilize any contractual agreements to build their own plan.

### Network Infrastructure

DIT will be responsible for all COR network infrastructure, including hubs, switches, routers and cabling. Any remote access needs must be met by using DIT's facilities, including secured dialup, VPN or other secured connectivity as defined by DIT. TPU agree to remove all modems and other devices/services that allow access into the network.

### Billing

DIT and TPU agree to provide billing assistance to each other when requested. Billing for services provided by DIT to DPU will be incorporated into the standard DIT billing.

Telecommunications services will be billed directly to TPU as cost plus undistributed overhead charges in the same manner as other City departments.

Technical support services will be provided without charge but prioritized below City requests except for critical problem situations such as facility or service outage.

For any application development services (Web, UNIX, Mainframe, PC), TPU shall incur costs for programming, analysis and machine costs for the development as detailed in the standard rate schedule published by DIT.

### Length of the MOA and Provisions for the Severance of the MOA

This is the complete and final expression of the parties to this MOA. Any modifications must be made in writing and signed by an authorized representative of each party. This MOA will remain in effect unless changed as follows:

- This MOA may be amended at any time as mutually agreed between DIT and TPU.
- DIT and TPU agree to make a reasonable effort to ensure that each is informed of any changes in their respective business environments that may require the termination of this MOA. Both parties agree to provide written notice of termination at the earliest opportunity, but not less than 30 days.

| **Third Party Users/Name of Organization** | **Department of Information Technology** |
|---|---|
| ____________________________ | ________________________________ |
| Director/TPU | Director, Information Technology |