Any request for remote access to The City of Lake Forest network must receive written approval through this request form. See City Administrative Directive 2-4a Use of Personal Mobile Devices (BYOD).

# REQUESTOR

Requestor

Sponsoring

Department

 Requestor Type Exempt Employee (No Overtime) Vendor/Contractor

 Non-Exempt Employee (Overtime) Elected/Volunteer

# ACCESS TYPE REQUESTED

 Smartphone/Tablet Synchronization VPN with File Access (Userhome, Usergroups, Shared)

Other

List Device(s) Type (Required if requesting Smartphone/Tablet Synchronization)

List Other Request

# TERMS OF SERVICE

R

EMOTE

A

CCESS

R

EQUEST

1. The Requestor is subject to the terms set forth in the City’s Administrative Directive 2-4a Use of Personal Mobile Devices (BYOD).
2. The Requestor is responsible for ensuring their Internet Service Provider (ISP) is in proper working order, installing any required software, and paying associated fees. By using Remote Access, connected devices are a de facto extension of the City’s network, and as such are subject to the same rules and regulations that apply to the City’s owned equipment.
3. The Requestor shall hold the City including the Information Technology (IT) Division harmless for any subsequent errors of hardware or software as a result of Remote Access.
4. Unauthorized users are not allowed access to the City’s network or data.
5. All computers connected to the City’s internal networks via Remote Access or any other technology must use the most updated and active anti-virus.
6. Requested VPN Remote Access will force all traffic to and from the device over the Remote Access tunnel. All other traffic will be dropped. Simultaneous access of a home network and the City network (Split Tunneling) is not permitted; only one network connection is allowed.
	1. The Remote Access gateways will be set up and managed by the City’s IT Division.
	2. Remote Access VPN will be automatically disconnected from the City's network after thirty minutes of inactivity. Artificial network traffic (pinging) are not to be used to keep the connection open.
	3. Remote Access VPN is limited to an absolute connection time of 24 hours.

[CONTINUED]

1/2

1. Vendor/contractor violations of network security are prohibited and may result in criminal and civil liability.
2. Vendors/contractors will cooperate with law enforcement if a criminal violation is suspected. Examples of security violations include, without limitation:
	1. Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the City’s IT Division.
	2. Unauthorized monitoring of data or traffic on any network or system without express authorization of the City’s IT Division.
	3. Interference with service to any user, host or network including, without limitation; mail bombing, flooding, and/or deliberate attempts to overload a system and broadcast attacks.
	4. Forging of any TCP/IP packet header or any part of email header information.
	5. Sending unsolicited mail messages including without limitation, commercial advertising and informational announcements.
	6. A user shall not use another site's mail server to relay mail without the express permission of the site.

# REQUESTOR ACKNOWLEDGEMENT

By submitting this request, Requestor is agreeing to these Terms of Service

Requestor Signature

# APPROVAL

Dept. Director

Approved

R

EMOTE

A

CCESS

R

EQUEST

 Approved Approved with Revisions (see below) Denied(see below )

Assistant Director IT or

Finance/IT Director

HR Director

(If Non-Exempt Employee)

2/2