CITY OF
VANCOUVER

File No.: 04-1000-20-2020-188

June 4, 2020

s.22(1)

Dear s.22(1)

Re: **Request for Access to Records under the Freedom of Information and Protection
of Privacy Act (the "Act")**

I am responding to your request of March 13, 2020 for:

1. **A list of all the URL categories blocked on the City network, with examples of
websites under each of the categories, and**
2. **Additional instructions to City employees regarding responsible website use.**

   Date Range: September 1, 2019 to March 20, 2020

All responsive records are attached.

Under section 52 of the Act, and within 30 business days of receipt of this letter, you may ask
the Information & Privacy Commissioner to review any matter related to the City's response to
your FOI request by writing to: Office of the Information & Privacy Commissioner,
info@oipc.bc.ca or by phoning 250-387-5629.

If you request a review, please provide the Commissioner's office with: 1) the request number
(#04-1000-20-2020-188); 2) a copy of this letter; 3) a copy of your original request; and 4)
detailed reasons why you are seeking the review.

Yours truly,

Cobi Falconer, FOI Case Manager, for

[Signature on file]

Barbara J. Van Fraassen, BA
Director, Access to Information & Privacy
Barbara.vanfraassen@vancouver.ca
453 W. 12th Avenue Vancouver BC V5Y 1V4

*If you have any questions, please email us at foi@vancouver.ca and we will respond to you as soon as possible. Or you can call the FOI Case Manager at 604.871.6584.

Encl.

:kt

Request #1
A list of all the URL categories blocked on the City network, with examples of websites under each of the categories (September 1, 2019 – March 20, 2020)

The following categories are current being blocked on the Internet egress firewall:

URL Category	Description and Example
Command and Control	URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data. Examples:N/A
Hacking	Sites relating to the illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs, how-to-advice and/or tips that may result in the compromise of networks and systems. Also includes sites that facilitate the bypass of licensing and digital rights systems. Examples: www.hackspc.com www.hackthissite.org
Malware	Sites containing malicious content, executables, scripts, viruses, trojans, and code. Examples: N/A
Phishing	Seemingly reputable sites that harvest personal information from its users via phishing or pharming. Examples: N/A

Note: above descriptions and examples taken from the firewall vendor's website:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

Request #2

Additional instructions to City employees regarding responsible website use.

City Employees are required to abide by City of Vancouver Policies. Policies related to Internet access include:

Computing and Telecommunications Facilities - General:
https://policy.vancouver.ca/ag01501.pdf

Computing and Telecommunications Facilities - Internet Usage
https://policy.vancouver.ca/AG01504.pdf