OLG CORPORATE POLICY

TITLE: **Viruses & Malicious Code**

POLICY #: **CP-04-05-012**

OWNER: **IT Risk Management and Compliance**

STATUS: **Final**

OLG Internal

TITLE: Viruses & Malicious Code

POLICY #: CP-04-05-012

OWNER: IT Risk Management and Compliance

STATUS: Final

Table of Contents

OLG Internal

TITLE: Viruses & Malicious Code

POLICY #: CP-04-05-012

OWNER: IT Risk Management and Compliance

STATUS: Final

PURPOSE

The intention of this policy is to protect Ontario Lottery and Gaming Corporation (OLG) Information Systems and data from damage caused by infections from computer viruses, worms, Trojan horses and other malicious code (malware).

All potential entry points for viruses and malicious code must be addressed to properly protect the OLG Enterprise environment from malware. This includes systems that provide multiple and redundant levels of protection at the workstation, server, and network infrastructure tiers.

APPLICATION AND SCOPE

All OLG employees who have access to OLG computer workstations, PCs, local area networks, and client/server systems.

DEFINITIONS

Employee(s): Includes full-time, contract, part-time, and temporary employees, and those employed by others to perform work or are granted access to OLG information technology resources**.**

Malicious Code/Malware Detection and Screening: Any unauthorized program that replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. Viruses, worms, and Trojan Horse programs are different categories of malicious code. Malware may have attributes of more than one category, such as a worm that deletes files and spreads itself to other users.

Virus: A malicious program that inserts some or all of its own code into another file. “Infected” files can be program files, system files, or data files that contain executable content.

Worm: A malicious program that has the ability to distribute itself to other users or computers across a network, typically via email.

Trojan Horse: A malicious program that poses as (or is hidden in) a useful or fun program, but actually performs malicious activity, such as destroying data.

Virus Detection Software: Antivirus (or "anti-virus") software is a class of program that searches hard drive and floppy disks for any known or potential viruses.

OLG Internal

Small-Scale Systems: Examples include internal servers, FTP servers, mail servers, intranet servers, and desktop machines (with the exception of mainframe and other large-scale systems)

REQUIREMENTS

1. General

1.1. Computer viruses must be eradicated as soon as possible in order to limit serious damage to OLG computers and data. Approved OLG anti-virus systems minimize and prevent damage to OLG data files and software, and record information to prevent and detect re-infection.

1.2. All OLG computer users are responsible to report virus infections and take the appropriate action to protect OLG systems.

1.3. Policy violations will be dealt with severely, up to and including termination of employment depending upon the particulars of the violation.

2. Detection Systems

2.1. Malware detection and screening software must be installed and enabled on all OLG small-scale systems so that users and administrators can be alerted to suspected virus infections.

2.2. All incoming and outgoing email messages and file attachments must be scanned and cleaned of viruses.

3. Non-Standard Computers

3.1. Every OLG employee who examines, processes, or stores OLG information using a non-standard computer must install and regularly run the most current version of an OLG-approved virus detection software package.

3.2. Authorization is required from Departments heads prior to an employee bringing their own personal computers, computer peripherals, or computer software into OLG facilities. All exceptions must be approved by the OLG IT Information Security Office.

4. Software Testing Prior to Use

4.1. All software must be tested to ensure that they are free of viruses on a stand-alone system before being used on OLG Systems in the production, development, or testing environments.

5. User Responsibilities

5.1. If users suspect a computer virus infection, they must immediately shutdown the involved computer, disconnect from the network, and call the OLG IT Service Centre.

5.2. Users are prohibited from attempting to eradicate a computer virus from their system unless explicitly instructed by the OLG IT Service Centre or the OLG Information Security Office.

5.3. Users must not disable or uninstall approved virus checking programs on any OLG equipment.

6. Unauthorized Software Use Prohibited

6.1. The installation or use of any unauthorized software programs on OLG equipment is not permitted. Unauthorized software includes any externally provided software from a person or organization other than a known and trusted supplier.

6.2. The downloading of software programs (not including data) from the Internet, dial-up electronic bulletin board systems, or any other systems outside of OLG is not permitted. OLG employees must comply with restrictions outlined in CP-04-05-001: Acceptable Use Policy.

7. Virus Handling Prohibited

7.1. Employees must not write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or hinder the performance of or access to any OLG computer, network, or information.

8. Overloading Computing Resources

8.1. Any program or process that may overload system resources or interfere with OLG business activities, such as computer worms or internet-based games, is considered malware, and must not be run or written on any computer program or process.

9. Sending Files to Third Parties (Excluding Email)

9.1. Any suspected incident of account or password compromise must be reported to the IT Security Office and all passwords must be changed immediately.

OLG Internal

10. Email Attachments

10.1. OLG authorized virus detection software is required to block certain types of electronic mail file attachments from entering the OLG network from external hosts before the attachment is opened or executed.

10.2. Only electronic mail attachments that are expected from a known and trusted sender may be opened.

POLICY OWNER

Queries concerning this policy should be directed to the IT Information Security Office.

RELATED POLICIES AND PROCEDURES

- CP-04-05-001: Acceptable Use Policy

TITLE: Viruses & Malicious Code

POLICY #: CP-04-05-012

OWNER: IT Risk Management and Compliance

STATUS: Final

REVISION / REVIEW HISTORY			
Date	**Requested By**	**Updated By**	**Summary of Revision**
10/10/2006	Stephen Madden, Executive Director, IT Risk Management and Planning	Dan O'Connor, IT Security Assessment Manager	New policy
30/11/2008	IT Security Assessment Manager	IT Security Assessment Manager	Annual Policy review
21/11/2009	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Dec 2010	IT Security Office	IT Security Office	Annual Policy Review (no updates)
Dec 2011	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2012	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Oct 2013	Corporate Policy Services	Corporate Policy Services	Reformat of policy template - AODA requirement
Nov 2013	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2014	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Dec 2015	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
Nov 2016	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
July 2017	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
July 2018	Annual Policy Review	IT Security Office	Annual Policy Review (no updates)
August 2019	Annual Policy Review	IT Security Office	Annual Policy Review

OLG-Internal

TITLE: Viruses & Malicious Code

POLICY #: CP-04-05-012

OWNER: IT Risk Management and Compliance

STATUS: Final

Sept 2021	Annual Policy Review	IT Security Office	• Annual Policy Review (no updates)

APPROVERS		
Department Approver	**Authorized Signature**	**Date**
Stephen Madden, Sr Director, Security Architecture & Standards	Stephen Madden	March 30 2007

EC / VP / BOARD OF DIRECTORS APPROVAL	
Approved By	**Authorization Date**

OLG Internal