REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

TO Live

Cybersecurity Policies

Date: September 11, 2023
To: Finance & Audit Committee and the Board of Directors of TO Live
From: President and Chief Executive Officer

REASON FOR CONFIDENTIAL INFORMATION

This report involves security of the property of the Board.

SUMMARY

This report provides an update on TO Live's cybersecurity controls and risks.

RECOMMENDATIONS

The President and Chief Executive Officer recommends that the Board of Directors of TO Live:

1. Approve new and updated cybersecurity policies 501 through to 510, as attached in Confidential Attachment 1.
2. Direct that Confidential Attachment 1 remain confidential as it involves security of the property of the Board.

FINANCIAL IMPACT

There is no financial impact at this time.

DECISION HISTORY

This is a new initiative.

COMMENTS

With continued focus on cybersecurity, TO Live is moving ahead with both new and updated cybersecurity policies, as noted in the summary below:

Cybersecurity Policies Update Summary

Policy #	Name	Purpose	Comments
501	Security Awareness and Training	Introduces new requirements that Security Awareness and Training is mandatory for all staff.	
502	Personal Passwords	Documents the personal password policy at TO Live and steps to be taken for any suspected account compromise.	Replaces TO Live Operational policy #106
503	Personal Computers	Updated policy outlining the roles and responsibilities that must be followed for using personal computers.	Replaces TO Live Operational policy #106
504	Mobile Device Management	Introduces new requirements that all mobile devices, including BYOD, are to be managed by TO Live's Mobile Device Management platform.	Replaces TO Live Operational policy #108
505	Credential Management	Documents the requirements for how TO Live should be creating and managing credentials throughout its on-premises and cloud.	
506	Access Management	Reiterates the necessary security rights and responsibilities that should be undertaken and reviewed before granting access for TO Live data and platforms.	
507	Critical Infrastructure	Introduces the requirements that should be met before anyone can access areas of critical infrastructure at TO Live.	

Policy #	Name	Purpose	Comments
508	Vulnerability Management	Outlines procedures which should be implemented and followed for accessing vulnerability risks with TO Live platforms both on-premises and cloud based.	
509	Cloud Security	Outlines the requirements and responsibilities that Cloud Security Providers must be able to provide to TO Live to ensure our data integrity and data security.	
510	Electronic Monitoring	Outlines what TO Live monitors electronically.	

CONTACT

William Milne
Vice President of Finance & Administration
T: 416-368-6161
William.Milne@tolive.com

David McCracken
Director of Information Technology
T: 416-368-6161
David.McCracken@tolive.com

SIGNATURE

Clyde Wagner
President & CEO

ATTACHMENTS

Confidential Attachment 1 - TO Live Cybersecurity Policies