JEWISH COMMUNITY FOUNDATION OF CALGARY ("JCFC")

Cyber Security Policy

Preamble:

The JCFC engaged Zacs computers audio and video to complete a cyber security vulnerability assessment which was completed as of January 18, 2024.

The JCFC's primary software for maintaining private and confidential software is Community Suite offered by Foundant Technologies ("Foundant"). Foundant completes a Type II SOC 2 Report On Controls Relevant To Security on an bi-yearly basis. The most recent audit covered the period February 16, 2022 to February 15, 2023 and was issued by their independent auditor Linford & Company LLP on March 16, 2023. In the interim the JCFC has received a letter from Chris Dahl, President, Foundant dated August 28, 2023 stating in part the following:

"I'm not aware of any material changes in our control environment that would adversely affect the opinion reached by L&C in the SOC 2 Report. Material changes are those that would require disclosure to L&C as our auditor in the process of their performance of the work required To Produce the Type II SOC 2 report."

ZACs has reviewed the "Security" summary provided by Foundant with respect to their protocols. The protocols outlined therein without system verification provide high security for data protection.

<u>JCFC Computer Systems & Hard Files</u>

Internal security controls are as follows:

- access to computers are protected by password.
- all electronic files containing sensitive, confidential and private data are password protected.
- third-party software systems containing sensitive, confidential and private data are accessed by password. Two step verification is utilized as available.
- Passwords must be a minimum of eight characters in length containing a minimum of one upper and lowercase letter and a minimum of one special character (#, @, $, ?, &, etc.)
- passwords must be input when computer systems and/or files containing sensitive, confidential and private data are accessed. Passwords are not to be embedded/saved for ease of access.
- computers and/or files are to be closed when not in active use.
- Hard files containing sensitive, confidential and private data are stored in locked cabinets.

- Hard files containing sensitive, confidential and private data that are not required are shredded.

JCFC Sensitive, Confidential and Private Data Stored on External Devices/Locations.

- access to external computers are to be protected by password.
- all electronic files containing sensitive, confidential and private data are password protected. Passwords must be a minimum of eight characters in length containing a minimum of one upper and lowercase letter and a minimum of one special character (#, @, $, ?, &, etc.)
- third-party software systems containing sensitive, confidential and private data are accessed by password. Two step verification is utilized as available.
- passwords must be input when computer systems and/or files containing sensitive, confidential and private data are accessed. Passwords are not to be embedded/saved for ease of access.
- computers and/or files are to be closed when not in active use.
- Files that are not required to be maintained on external computers are to be immediately deleted.
- Hard files containing sensitive, confidential and private data that are not required are to be shredded.

Policy Review

This policy will be reviewed every 3 years or as required.

- **Cyber Security Policy Approved by the JCFC Board January 24th, 2024**