Development Corporation for Israel Member FINRA
DATA SECURITY STATEMENT

OUR COMMITMENT TO CLIENTS

Development Corporation for Israel (DCI) takes the security of our client's personal and financial information very seriously. Our data security policies and procedures are designed to protect our clients' personal and financial information.

We protect our clients' sensitive information by utilizing the following:

• ***Training:*** Every DCI employee is required to understand and acknowledge DCI's data security policy. Employees receive training on data security at least annually.

• ***Encryption:*** DCI provides a secure website and app to log in to apply for accounts, access clients' accounts and purchase bonds. You can verify that security is enabled by looking for the padlock or key icon on your browser.

• ***User ID and Password:*** To access your purchaser account online, you must provide a unique ID and a password. Your password must meet certain requirements in order to ensure that it is a strong and adequately secure one. DCI representatives will not ask you over the phone or by email or text message to provide your online password.

• ***Session Timeout:*** DCI uses a time out feature to log clients off their accounts after a specified period of inactivity. This reduces the chances of your information being compromised if you leave your computer unattended.

• ***Identity Verification Process:*** DCI verifies the identities of its clients at account-opening using third-party verification services or through documentary evidence such as passports or drivers' licenses. This process is designed to ensure that the person opening the account is who they claim to be. When you contact us, we will verify your identity before discussing account information or before completing a transaction.

• ***Our Defenses:*** DCI's purchaser website is protected by firewalls and other intrusion detection mechanisms. We continuously monitor our defense systems to detect any attempted intrusions or unauthorized connections and test periodically to validate our security defenses.

WHAT YOU CAN DO

DCI has taken important steps to protect your information. However, it is important that our customers take an active role in protecting their electronic devices and their log-in information.

We ask that you review the guidance below which includes some general guidelines and best practices:

• ***Protect your password:*** Never share your password with anyone. We also recommend you change your password on a regular basis. If you feel that your password has been compromised, change it and notify us right away by calling or emailing Client Support at 888.519.4111 or client.support@israelbonds.com

• ***Use Antivirus and Firewall Software:*** We recommend you install an antivirus product on your computer and update it to ensure that your system is checked for the latest viruses regularly.

• ***Log off the Website:*** When you have finished your transactions, it is important that you click the "log off" link. If you are using a public personal computer it is recommended that you also close the browser when finished. Do not use public or unsecured Wifi to access your account.

• ***Beware of Phishing and Clicking Links:*** We will not send you emails or text messages asking for sensitive information such as social security numbers or for your password. Be very careful before clicking on links or opening attachments that you receive by email. If you receive an email that appears to be from us but you have any concerns about its validity, do not click on any links or open any attachments. Contact your registered representative or Client Support first at 888.519.4111 or client.support@israelbonds.com