Combined Jewish Philanthropies

Securing Business Operations in a Remote Environment

March 26, 2020
Having a Clearly-defined Plan

Important to:

– Establish new operating rhythms.
– Keep lines of communications open.
– Maintain regular business operations.
– Emphasis your cybersecurity policies.
– Be aware of ever-changing regulations.
Establish New Operating Rhythms

Establishing a New Normal:

• Hold regularly-scheduled meetings virtually.
• Define what remote working will look like by outlining expectations and address employee concerns.
• Advocate for personal and professional separation;
  – honor the end of the work day and urge your staff to do the same.
• Things are going to take longer at first. You and your staff are getting used to a new normal. Take comfort that everyone is experiencing the same thing.
• You may need to adjust and make exceptions to guidelines. Employees who look after young children or older adults, or who may be ill themselves, may not be able to work the same hours.
Keep Lines of Communications Open

- Communicate internally and externally promptly and clearly.

- Keep employees updated as your organization’s policies change with the constantly-changing restrictions.

- Ask managers to initiate communications in whatever mode is preferred by staff (e-mail, instant messaging, video conference, phone, etc.).

- Outline a crisis plan that informs the communication flow and that it provide employees with the confidence to react appropriately.
Maintaining Business Operations

Keeping Business Operations Moving:

• Identify staff that can perform their duties remotely with little business interruption.

• Identify staff that need to be at the place of work to ensure business continuity; for example: mailroom, security, facilities, finance staff.

• Identify staff who will now have capacity in their work schedules as a result of cancellations and closings. Is there work that can be redeployed?

• Paying employees their salaries is important and it is the law. Have procedures in place to make sure you can pay your staff timely and accurately as outlined by the Department of Labor.
Maintaining Business Operations (Cont’d)

Transaction Processing:

- Confirm banking arrangements.
- Develop a process to review incoming mail.
- Encourage donors, members, and families to pay remotely by credit card using the organizations’ websites or sending electronic payments directly from their banks.
- Have dedicated staff whose responsibility is to deposit and record checks, while maintaining strong internal controls.
- Encourage vendors, consultants, and utilities to send invoices electronically.
- Utilize online banking and electronic payment methods to pay vendors, consultants, and utilities.
- Empathy, understanding, and the willingness to be flexible is key.
Maintaining Business Operations (Cont’d)

Other Considerations:

• If there are cash needs, determine what other sources are available.

• Review insurance policies in place for business interruption coverage; contact your insurer.

• Seek help from appropriate professional advisors.
Emphasize Your Cybersecurity Policies

Educate Your Staff of Phishing Scams:

• Ignore online offers for vaccinations for the COVID-19 virus - there are none.

• Make sure that your donations to aid relief for this outbreak go to a qualified charity - do your research.

• Do not use public wi-fi - use your mobile device hotspot instead, if necessary.

• Follow your existing cybersecurity policies and perform random phishing tests to ensure your staff is being diligent.
Examples to Identify Phishing

• Do not click on an unrecognized link.

• Do not provide personal or confidential information, such as your log-in credentials.

• Look for spelling errors and poor grammar.

• Look for a sense of urgency or a threatening tone - these are immediate red flags.

• Go to the source if something looks questionable. Call your boss, the bank, or whoever the source of the request is supposedly coming from.
Ever-changing Regulations

• The IRS' New Tax-filing Deadline is July 15, 2020.

• The U.S. government is extending the tax-filing **deadline** to July 15, a move meant to give taxpayers extra time to deal with their taxes amid the Coronavirus outbreak.

• Taxpayers now have an extra three months to both file and pay their taxes.

• The guidance does not change to filing requirements for corporate taxpayers; however, corporate taxpayers have until July 15, 2020 to make tax payments without penalties and interest.
Written Notices Are Required for Cancelled Fundraising Events:

• Nonprofits are required to provide a written notice to donors when a quid pro quo contribution is received in excess of $75.

• If these notices have already been provided for sponsorships and ticket sales for cancelled events, they will need to be reissued.

• Donors who elect not to receive a refund for their purchases of tickets or sponsorships will need to be informed that their contribution is no longer a quid pro quo contribution.
Ever Changing Regulations (Cont’d)

Notice needs to include:

• A statement that no goods or services were provided in exchange for the donation;
• The amount of the gift, or a description of a non-cash gift;
• The date of the donation;
• A statement that the organization is a 501(c)(3) organization;
• A statement that the letter does not contain tax advice; and
• A statement that they should consult their tax preparer.
Ever Changing Regulations (Cont’d)

FMLA and Paid Sick Leave Under the Families First Act:

• Small to midsize employers are required to provide 80 hours of paid sick leave to fulltime employees.

• Employees caring for a minor child are entitled to two-thirds of their average earnings for up to 10 weeks of emergency paid family and medical leave.

• On March 20, the U.S. Treasury Department, Internal Revenue Service (IRS), and the U.S. Department of Labor (Labor) announced that small and midsize employers can take advantage of two new refundable payroll tax credits, designed to immediately and fully reimburse dollar-for-dollar costs associated with providing Coronavirus-related leave to their employees.
Additional Resource: CJP Communal Security Initiative

Provides Free Security Support to Jewish Organizations in area, Including:

• Education & Training,
• Security Assessments,
• Consultations,
• Grant Support,
• Emergency Communications—Jewish Emergency Management System (JEMS)
• Law Enforcement Partnerships

CJP.org/CommunalSecurity for information
Questions?

Our contact information:

David Strong, CFO: davids@cjp.org

Carmela Caplain, VP, Finance: carmelac@cjp.org

Ted Penfield, AVP, Information Technology: tedp@cjp.org

Jeremy Yamin, AVP, Director of Security and Operations: CommunalSecurity@cjp.org