NNSC
NETWORK OF NONPROFIT SEARCH CONSULTANTS

Best Practices for Securing Your Firm's Sensitive Data

September 2020

Researched and authored by Sally Bryant, President & CEO of BRYANT GROUP, with input and advice from Doug Brush, cyber security expert, and Jeremy Zuther, "Mr. Computer"

As search firms, the information we gather is many times sensitive, private and confidential. Even if the firm is not gathering social security numbers, many times we do have documents including home address, personal cell phone, personal email, and possibly date of birth. In this age of millions of records being compromised on a continuous basis (~327 million recently through Marriott records, for example), it is important that we put proper measures in place to protect our candidates and our clients.

We have a responsibility to not only protect candidates' contact and personal information, but also to protect our clients by not allowing sensitive background and other information to become part of a record that later is made public through Freedom of Information Act (FOIA) actions.

The threats come in several forms, including hackers, viruses, and scams. Hackers can access a hard drive or even more likely, an email either in transit or email stored on a computer or on the email server.

Please note that this is a starting point for cyber security when delivering search services and should not be misconstrued as legal advice. For more specific information about protecting sensitive data, please reference the General Data Protection Regulation (GDPR).

General Cyber Security Recommendations:

- Use a password manager (like LastPass or 1Password) that will store all of your passwords. These programs also suggest passwords for use. (They create unique, random, combinations of letters/numbers/characters for each site which are harder to guess by unauthorized people.)
    - Do not store any work passwords in electronic "notes," Word documents, or other plain text methods that do not require a password.

    - Do not transmit any passwords in "clear text" such as in the body of an email. Services such as One Time Secret (https://onetimesecret.com/) are useful for sharing passwords when necessary.

    - Do not share your password manager password with anyone. If you share a password manager with your spouse, do not store company info on it; use a different password manager for company passwords and personal passwords.

- Do not leave your computer open/unlocked/accessible in any unsecure area. This includes hotels, airplanes, conference rooms, etc. Lock your computer screen when away and use a privacy shield when in public places.

- Do not allow "guest" users on your computer. Turn off the Guest User access function.

- If you use a shared file drive, ensure it is password protected and that each employee has their own password to access it.

- Do not use unsecured wifi (like those in hotels, airplanes and coffeeshops, for example). Use a personal Hotspot or other secure network.

- If you must use public wifi, invest in a virtual private network (VPN), which encrypts communications when on public wifi. Email is more vulnerable to breaching than the hard drive of a computer. The problem with public wifi is that, potentially, someone could access the computer and set up "man in the middle," thereby imitating a public wifi network (when actually the user is on the hacker's wifi network).

- Use different passwords for all accounts.

- Change passwords when known or suspected to be compromised.

- IT personnel sometimes will ask to "remote in" to fix something. This should only be allowed as a last resort and only with a trusted source.

  Note: To Encrypt a document at rest = password. To encrypt an email means the body of the email itself is not accessible.

Email:

- All employees using company email are required to use password-protected email through the company-designated provider.

- Via Outlook and the Office 365 platform, turn on Email encryption.

- Never ask for a Social Security Number or a Date of Birth for a candidate unless absolutely necessary. (For example, if needed for degree verification). If SSN or DOB are needed, gather the information by phone (voice, not text) after receiving a signed authorization from the candidate that the firm is allowed to receive this information. If this information is needed in writing, use DocuSign.

- Password protect candidate information packets, reference reports and other sensitive documents when sending electronically to clients.

- Sharing candidate information with third parties, including clients, degree verification centers and candidate employers (current and former), should be done through a secure link or a password-protected document. Adobe can password protect documents and Adobe Share allows the user to open a document via a link. Set link to expire in 48 hours.

- Use a password formula for documents that ensures consistency, but is different for each client. This password formula will be given out to authorized individuals verbally by the administrator and must be kept in complete confidence, and shared only when providing to an authorized third party. (Spouses and family members are not authorized third parties.)

- Because most data incidents happen when attackers gain access to email (and can download whole copies of mailboxes including all folders), firm employees must: 1) protect all confidential information in email using the above precautions, 2) consider carefully the content that is written and sent by email both internally and externally, and 3) store important documents on the hard drive and/or a 2-factor authentication Cloud backup (such as Carbonite).

- All employees will review and delete email on a monthly basis. All important documents should be stored on a hard drive, in the Cloud with password protection, and/or in hard copy. Deleting email requires "deleting" or "trashing" it and then "emptying" or deleting the trash.

- All employee and independent contractor computers must be password protected.

- Each employee/independent contractor may store company information on one desktop and one laptop only.

- All hard copy files should be stored in a home or office that is secure from unauthorized access. Unauthorized access includes family members of

employees and independent contractors.

- Do not download attachments from unknown sources. If you are not sure whether or not to download a file, call the IT department.

Documents:

- When receiving or creating a document with sensitive information, such as an authorization to conduct a background check or degree verification, use Adobe to redact all sensitive information prior to uploading documents to the candidate file in the database.

- Carbonite is a good system to use for storing backups of documents, as it has a 2 -factor authentication.

Sally Bryant joined BRYANT GROUP in 2007 and brings 30 years of experience in advancement management, consulting and recruiting, as well as achievements from the corporate sales arena and success in other entrepreneurial activities. She is also a member of NNSC.

***

*The **Network of Nonprofit Search Consultants** (NNSC) is a professional organization comprised of some of the leading nonprofit search consultants in the United States and Canada. NNSC provides a forum for executive search consultants to discuss best practices in the field of retained search services predominantly for nonprofit organizations and non-governmental organizations. Our mission is to reflect the goals of the nonprofit organizations we serve, as well as ensure that the best leadership is in place to meet the needs of a strong, vibrant nonprofit sector. For more information about NNSC or to find a search consultant to assist you, visit www.nnsc.org.*