IT EMAIL

POLICY

The Board recognizes email is an essential component of business communication; however, it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the Board's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

The purpose of this policy is to detail the Board's usage guidelines for the email system. This policy will help the Board reduce risk of an email-related security incident, foster good business communications both internal and external to the Board, and provide for consistent and professional application of the Board's email principles.

The scope of this policy includes the Board's email system in its entirety, including desktop and/or web-based email applications, mobile device applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the Board network.

This document is part of the Board's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

IT EMAIL

PROCEDURE

I. **Proper Use of Board Email Systems**

Users are asked to exercise common sense when sending or receiving email from Board accounts. Additionally, the following applies to the proper use of the Board email system.

A. **Sending Email**

When using a Board email account, email must be addressed and sent carefully. Users should keep in mind that the Board loses any control of email once it is sent external to the Board network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the Board avoid the unintentional disclosure of sensitive or non-public information.

B. **Personal Use and General Guidelines**

Personal usage of Board email systems is prohibited. Users should use Board email systems for business communications only.

The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

The user is prohibited from forging email header information or attempting to impersonate another person.

Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the Board may not be sent via email, regardless of the recipient, without proper encryption.

It is Board policy not to open email attachments from unknown senders, or when such attachments are unexpected. Report any suspicious or unknown email to the IT Helpdesk for review.

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this policy.

C. **Business Communications and Email**

The Board uses email as an important communication medium for business operations. Users of the Board email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from a Board account reflects on the Board, and, as such, email must be used with professionalism and courtesy.

D. **Email Signature**

An email signature (contact information appended to the bottom of each outgoing email) is recommended for all emails sent from the Board email system. At a minimum the signature should include the user's:

Name and Title
Board name
Phone number(s)
Fax number if applicable
URL for Board website

Email signatures may not include personal messages (political, humorous, etc.). The IT department is able to assist in email signature setup if necessary.

E. **Auto-Responders**

The Board recommends the use of an auto-responder (Out of Office Assistant) if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required. Staff authorized to use mobile devices are not required to use this feature if they are able to respond using their device.

F. **Mass Emailing**

The Board makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for communications (such as when communicating with the Board's employees), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is the Board's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the Board requires that email sent to more than twenty (20) recipients external to the Board have the following characteristics:

1. The email must contain instructions on how to unsubscribe from receiving future

emails (a simple "reply to this message with UNSUBSCRIBE" in the subject line will do). Unsubscribe requests must be honored immediately.

2. The email must contain a subject line relevant to the content.

3. The email must contain contact information, including the full physical address, of the sender.

4. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note: Emails sent to Board employees, existing customers, or persons who have already inquired about the Board's services are exempt from the above requirements.

G. **Opening Attachments**

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. The IT department places a header at the top of every email that originates outside of the Stark DD Network to alert employees that the email has indeed been sent from an outside source. This helps combat the growing threat of malicious spammers spoofing an email to look like it is coming from a Board employee. Users should:

1. Never open unexpected email attachments.

2. Never open email attachments from unknown sources.

3. Never click links within email messages unless he or she is certain of the link's safety.

The Board may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary. If there is any doubt about an email, link, or attachment, contact the IT Helpdesk for verification.

H. **Monitoring and Privacy**

Users should expect no privacy when using the Board network or Board resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The Board reserves the right to monitor any and all use of the computer network. To ensure compliance with Board policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

I. **Board Ownership of Email**

Users should be advised that the Board owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the Board and it may be subject to use for purposes not anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

J. **Contents of Received Emails**

Users must understand that the Board has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the Board may attempt to reduce the amount of this email that the users receive; however, no solution will be 100% effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor.

K. **Access to Email from Mobile Phones**

Many mobile phones or other devices, often called smartphones or tablets, provide the capability to send and receive email. The Board permits users to access the Board email system from a mobile device. Refer to the Mobile Device Policy for more information.

L. **Email Regulations**

Any email that contains information regarding a specific person(s) served must be kept according to the Board's records retention schedule.

M. Reporting of Suspicious Email

Any email that is the least bit suspicious should be reported to the IT Helpdesk immediately. The IT department will assist the user in determining if the email is legitimate or malicious and will direct the user what to do accordingly. A few minutes of investigation can prevent days worth of downtime and recovery in the event of an infection. Always error on the side of caution when receiving an attachment or link in an email.

II. **External and/or Personal Email Accounts**

The Board recognizes that users may have personal email accounts in addition to their Board-provided account. The following sections apply to non-Board provided email accounts:

A. **Use for Board Business**

Users must use the Board email system for all business-related email. Users are

prohibited from sending business email from a non-Board-provided email account.

B. **Access from the Board Network**
Users are prohibited from accessing external or personal email accounts from the Board network.

C. **Use for Personal Reasons**
Users are required to use a non-Board-provided (personal) email account for all non-business communications. The Board email system is for Board communications only. Users must follow applicable policies regarding the access of non-Board-provided accounts from the Board network.

III. **Confidential Data and Email**
The following sections relate to confidential data and email:

A. **Passwords**
As with any Board passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. Upon the recommendation from the HIPAA Privacy or Security Officer and at the discretion of the Superintendent, the Board may further secure email with certificates, two factor authentication, or another security mechanism.

B. **Emailing Confidential Data**
Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

The Board requires that any email containing confidential information sent external to the Board be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to the Board. When in doubt, encryption should be used.

Further guidance on the treatment of confidential information exists in the Board's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

IV. **Board Administration of Email**
The Board will use its best effort to administer the Board's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.

A. **Filtering of Email**
A good way to mitigate risk from email is to filter it before it reaches the user so that

the user receives only safe, business-related messages. For this reason, the Board will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the Board's IT security. No method of email filtering is 100% effective, so the user is asked additionally to be cognizant of this policy and use common sense and an abundance of caution when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the IT Manager.

B. **Email Disclaimers**

The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in the Board's risk reduction efforts. The Board requires the use of email disclaimers on every outgoing email, which must contain the following notices:

- The email is for the intended recipient only.
- The email may contain private information.
- If the email is received in error, the sender should be notified and any copies of the email destroyed.
- Any unauthorized review, use, or disclosure of the contents is prohibited.

An example of such a disclaimer is:

NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.

The Information Technology Department should review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.

C. **Email Deletion**

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the Board to store and backup unnecessary email messages. Email should be maintained according to the Board's records retention schedule.

However, users are strictly forbidden from deleting email in an attempt to hide a

violation of this or another Board policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

The Board must note and document here any applicable regulations or statutes that apply to email deletion.

D. **Retention and Backup**

Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

E. **Address Format**

Email addresses must be constructed in a standard format in order to maintain consistency across the Board. The Board format is:
LastnameFirstinitial@StarkDD.org

The intent of this policy is to simplify email communication as well as provide a professional appearance.

F. **Email Aliases**

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for Board email, as well as (often) the names of Board employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- techsupport@Boarddomain.com
- pr@Boarddomain.com
- info@Boarddomain.com

The Board requires the use of email aliases in all situations where an email address will be exposed to, or reachable by, the general public.

G. **Account Activation**

Email accounts will be set up for each user determined to have a business need to send and receive Board email. Accounts will be set up at the time a new hire starts with the Board, or when a promotion or change in work responsibilities for an

existing employee creates the need to send and receive email.

At times, email accounts may be given to non-employees, contractors, or other individuals authorized to conduct certain aspects of the Board's business. In these cases, the Board should consider designating the temporary or non-employee status of the account in the account name, such as:

• hrintern1@Boarddomain.com
• printern1@Boarddomain.com.
•companynameconsultant@Boarddomain.com

H. **Account Termination**

When a user leaves the Board, or his or her email access is officially terminated for another reason, the Board will disable the user's access to the account by password change, disabling the account, or another method. The Board is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the Board.

I. **Storage Limits**

As part of the email service, email storage may be provided on Board servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IT Manager. Storage limits may vary by employee or position within the Board.

V. **Prohibited Actions**

The following actions shall constitute unacceptable use of the Board email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the Board email system to:

• Send any information that is illegal under applicable laws.

• Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of Board executives in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities and has been approved by the Superintendent or designee.

• Send any emails that may cause embarrassment, damage to reputation, or other harm to the Board.

• Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude,

harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

• Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.

• Make fraudulent offers for products or services.

• Attempt to impersonate another person or forge an email header.

• Send spam, solicitations, chain letters, or pyramid schemes.

• Knowingly misrepresent the Board's capabilities, business practices or policies.

• Conduct non-Board-related business.

The Board may take steps to report and prosecute violations of this policy, in accordance with Board standards and applicable laws.

A. **Data Leakage**

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the Board's control of its data.

Unauthorized emailing of Board data, confidential or otherwise, to external email accounts for the purpose of saving this data external to Board systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from Board systems.

The Board may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IT Manager.

B. **Sending Large Emails**

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The Board asks that the user limit email attachments to 10Mb or less.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

VI. **Enforcement**

This policy will be enforced by the IT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the Board may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

Definitions

Auto Responder - An email function that sends a predetermined response to anyone who sends an email to a certain address such as Out of Office Assistant. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate - Also called a "Digital Certificate" is a file that confirms the identity of an entity, such as a Board or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage - Also called data loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email - Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a Board or between companies.

Encryption - The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Mobile Device – Is a portable device that can be used for certain applications and data storage. Examples are Tablets or Smartphones.

Password - A sequence of characters that is used to authenticate a user to a file, computer, network, or other device; also known as a passphrase or passcode.

Spam – Is unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Smartphone - A mobile telephone that offers additional applications such as internet access and email.

Two Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.