San Francisco Department of Public Health
Office of Compliance and Privacy Affairs

City and County of San Francisco
London N. Breed, Mayor
San Francisco Department of Public Health
Grant Colfax, MD, Director of Health

Email Auto-Encryption Exception
User Agreement

Version: November 18, 2022

The City and County of San Francisco utilizes e-mail encryption software to ensure our email transmissions are private and secure. In situations where the encryption software's security algorithm deems it necessary, it automatically encrypts outgoing email messages.

There may be cases where auto-encryption interferes with SFDPH business without providing needed security or privacy benefits. In these cases, the Office of Compliance and Privacy Affairs (OCPA), with input from the SFDPH Chief Information Security Officer, is willing to provide exceptions to the SFDPH Data Encryption Policy and disable auto-encryption feature for specific email accounts.

To request an exception from auto-encryption, please complete the following:

I confirm that the following are true:

☐ 1. My job duties do not require me to send information defined as Confidential via the SFDPH-issued email address for which I am requesting an exception.

Confidential information: Information that should be restricted such as Protected Health Information (e.g. patient name, diagnosis), personal information (e.g. social security number, date of birth) or employee information (e.g. human resources records).

☐ 2. My job duties require me to interact with the public and/or external organizations, and auto-encryption has hindered my ability to communicate in a timely and effective manner.

☐ 3. I will only use email auto-encryption bypass capabilities in situations where appropriate. I understand that misuse of auto-encryption bypass could lead to disciplinary action consistent with the severity of the incident, which may include, but not be limited to:
- Loss of access privileges to information resources
- Termination of employment
- Other actions as deemed appropriate by the joint determination of the Human Resources Department, the Information Security Office or the CIO.

☐ 4. When the business need for an exception no longer exists (change in job duties or new position within SFDPH), I will alert OCPA to reinstate auto-encryption on my email account within 48 hours.

Office of Compliance and Privacy Affairs, San Francisco Department of Public Health
101 Grove Street, Room 330, San Francisco, CA 94102
Office email: compliance.privacy@sfdph.org – Office telephone: 415-554-2787 – Office fax: 415-554-2845
Confidential Compliance and Privacy Hotline: 1-855-729-6040 toll-free
Calls may be made confidentially and anonymously – Always remember: SFDPH has a non-retaliation policy

Please briefly summarize your situation and how encryption is interfering with your work:
(Requests will not be processed if this section is not completed.)

By signing this document, I state that I have a legitimate need for an exception to the auto-encryption email function, I attest that my answers to the statements above are true to the best of my knowledge, and I agree to comply with the terms and conditions above.

Name (Signature): _____

Name (Print):_____

Class # & Job Title: _____

Program/Division: _____

Privacy Training Completion Date: _____

Date: _____

Please have your supervisor complete the following:

By signing this document, I state that to the best of my knowledge, the needs stated above for an exception to this policy are true.

Supervisor Name: _____

Supervisor Signature: _____

Please return this form via email to:

datasharing@sfdph.org

OCPA Approver:

Approval date: