EPHEMERAL COMMUNICATION GUIDE

Part 1: Setting Internal Policies

The goal of this document is to provide customers with high-level guidance[1] on how ephemeral communication technology ("ET") can be operationalized within a business or organization. Specifically,

[1] *Note: This guide does not constitute legal advice. We recommend that you consult with your information management and legal professionals to ensure proper data expiration periods are applied against the appropriate data retention periods.*

Part 1 of this document aims to highlight key considerations of organizations that are considering the use of ET for enhanced security and privacy of their business. Part 2 demonstrates a sample communications standard to use as a starting point, and Part 3 provides reference materials for additional reading.

Why Ephemeral Communication Tools Belong in the Workplace

Given the unrealistic expectation that current end-point security techniques will be successful in combatting persistent adversaries in the digital age, it is reasonable and necessary for organizations to use secure and ephemeral communication tools such as Wickr.

The use cases for secure and ephemeral communications tools are countless but obtain increased relevance in situations where a breach of security and confidentiality between employees and trusted partners will have a material impact on the organization.

Key Considerations for Using Wickr Products

- **Compliance**
- **Document Retention**
- **Data Classification**
- **Internal Policies**

1) Consider Compliance First

The jumping off point for using ET is to ensure that compliance requirements are met. If there is a requirement[2] for your organization or industry to retain communications, or if you are under litigation hold (or have a reasonable anticipation of litigation[3]), you must ensure that you can comply with the retention requirements by selecting the correct Wickr product to use. Wickr Enterprise is a robust product which was designed to allow administrators to enforce preservation/retention periods across a group of users whereas Wickr Pro should be limited to organizations who do not have or anticipate having retention requirements for compliance or other needs. If legal preservation becomes required through litigation hold during the use of Wickr Pro, use of the product by those subject to such holds can be restricted to subject matter not under the hold. Alternatively, administrators may consider having the affected users pause use of the product until the hold period has passed.

2) Consider Document Retention Policies and Standards

Employees and stakeholders should use ET in conjunction with appropriate data retention policies to send confidential communications. Most working-level communications should never be stored for security purposes.

[2] Such requirements may be contractual or, more frequently, statutory.

[3] "Reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation." The Sedona Conference Commentary on Litigation Holds: The Trigger & The Process, The Sedona Conference®, Vol XI, page 269 (2010).

Organizations that do not have document retention requirements should default to risk reduction and minimize the amount of information that is retained and therefore could be breached. Organizations that have requirements to maintain working-level documents and communications, for example, will need to tailor their retention periods accordingly.

Wickr Pro can be administered to allow for up to one year of retention of files and communications for long-term projects. Shorter time frames may be appropriate where long-term retention is not required. Specific ephemerality settings can be determined on a team-by-team and project-by-project basis. Wickr is primarily a communication and data transport tool and files are stored as part of conversations in an unstructured or searchable fashion. If you currently employ a document management or enterprise content management schema with secure repositories, it should be a matter of policy to save any files transported via Wickr to those existing systems as you policy would already dictate.

Wickr Enterprise allows organizations to selectively log communication sessions to a secure customer defined data store, when required. If permanent retention is required for archival purposes such as FOIA, e-discovery & auditing purposes, archival.

3) **Consider Data Classification Systems**

A well-planned data classification system is of particular importance for risk management, legal discovery, and compliance. Written procedures and guidelines for data classification should define what categories and criteria the organization will use to classify data and specify the roles and responsibilities of employees within the organization regarding data stewardship. Once a data-classification scheme has been created, security standards that specify appropriate handling practices for each category and storage standards that define the data's lifecycle requirements should be addressed.

4) Consider Your Company's Internal Policies Around Individual Expectations of Privacy

In the ever-digital age of communication, it is up to each organization to clearly and transparently ensure employees know what their expectation of privacy should be when using any employer-owned system, tool or device. This is particularly important in "bring your own device" (BYOD) enterprises where there is a blurred line between the personal and the professional. Wickr has chosen to emphasize security, privacy and transparency within its products and that is reflected within its company policies. Therefore, we find it helpful to have ensure that your BYOD policy aligns with this technology.

Summary

Secure and ephemeral communications tools need to be considered within the larger infrastructure of cybersecurity measures. In any organization, it is necessary to train employees and stakeholders on the

proper ways to communicate sensitive information, both inside and outside of the organization. The ever-growing sophistication of cyberattacks and adversaries dictate the need for an ever-evolving and adaptable system to minimize the impact cyberattacks have on core business operations.

As explained in the National Law Review, "[I]nformation security is one key reason to consider adopting encrypted ephemeral communications in corporate settings. As an initial matter, use of ephemeral communication tools can minimize the breadth of exposure following a data security incident. If a company has a policy in place that calls for the routine and periodic expiration and deletion of information, that information is simply not available on the system to be "hacked." Further, the use of ephemeral communication tools (and public disclosure of that use) may also deter potential incursion attempts as some sensitive and valuable information will no longer exist. This deterrence may be particularly valuable given the increased shareholder and investor focus on data security, a dramatic uptick in data breaches, and the potential cost of a data security incident[4]."[5]

Wickr Pro and Wickr Enterprise are the go-to products of choice for those entities that understand, or are coming to terms with the information risks associated with leaving communications unprotected.

[4] A 2016 Ponemon Institute study calculated that the average cost of a data breach is $4 million per company, with the loss or theft of sensitive data reaching $158 per record.

[5] https://www.natlawreview.com/article/key-considerations-adopting-ephemeral-communications-tools

EPHEMERAL COMMUNICATION GUIDE

Part 2: Sample Policy[6]

[6] *Note: This is an abstract from the communication standard section of Wickr's own information governance policy.*

Secure Communication Standard

Version: 1.0
Date of Last Review/Approval: TBD
Approved By: Risk Committee
Data Classification: Internal Use Only

Table of Contents

Introduction

There are many means of electronic communication available to people today. However, improper use of communication tools and services can pose significant security, legal, and privacy risks to our organization. It is each employee's responsibility to understand what they are communicating (Data Categorization) and the approved means to communicate it.

Scope

This standard covers the use of communication and collaboration tools and applies to all full-time and part-time employees, contractors, consultants, temporary workers, and other workers including all personnel affiliated with third parties ("Associates"). It addresses communication and data transfer but does not address data storage and access or other security standards.

Data Categorization

The following are the classifications all data (communications, files, other mediums) must fall into. It is the responsibility of the data creator to properly classify the data and communicate that classification so that all parties can adhere to the policy related to it. It is the responsibility of the business unit manager to ensure their staff understand the classification policy and the business unit manager to police it's proper use.

- Confidential: Highly sensitive corporate and customer data that if disclosed could put the organization at financial or legal risk.
    - Example: Customer information under NDA, nonpublic board communications, incident response communications, Merger and Acquisition discussions, nonpublic communication from VP and above, file transfer of all nonpublic information outside corporate network (Email is not appropriate for confidential data unless specifically stated from legal in writing).
    - Approved Tools:
        - Wickr: Wickr will be used for all confidential data messaging, voice conversations, and file transfer to ensure only authorized intended access of participants, and that information is not retained or archived. Maximum expiration to be set at 30 days with burn on read left to the discretion of the sender (off). *Note*: Compliance and legal needs may require data retention, in which case Wickr Compliance will be configured to meet those needs.
- Restricted: Sensitive internal data that if disclosed could negatively affect operations.
    - Example: Contracts with third-party suppliers, employee reviews
    - Approved Tools:
        - Wickr: Will be used for all restricted data life cycle for conversations, file transfer, to ensure only authorized intended access of participants, and that temporary information is not retained or archived. Maximum expiration to be set at 60 days with burn on read left to the discretion of the sender (off).
- Internal Only: Internal data that is not meant for public disclosure.
    - Example: Sales contest rules, organizational charts

- Approved Tools: Wickr, Company email, Corporate internal social blogs and ticketing systems, Corporate and personally owned fixed and mobile telephony systems and mobile SMS

- Public: Data that may be freely disclosed with the public.
  - Example: Contact information, price lists, announcements, support communications
  - Approved Tools: Wickr, Company email, Corporate internal social blogs and ticketing systems, Corporate and personally owned fixed and mobile telephony systems and mobile SMS

Directives

a. Only approved communication tools are authorized for conducting Wickr-related business. Tools are approved for use with specific categories of information according to their security capabilities. See Appendix A for a list of approved communication tools.
b. Communication tools shall be configured and used in a manner that maximizes their security effectiveness.
   - Options to reduce the time that content is retained must be carefully considered on a conversation-by-conversation basis and employed by default to secure information from potential breaches, taking into account any required retention periods such as a litigation hold.
   - Options for user authentication and verification should be utilized to reduce the risk of communicating with unintended parties.
   - Options to obscure or remove on-screen content should be utilized to secure information from potential onlookers.
c. Use of personal email or messaging systems[7] to store or transmit non-public Wickr-related information is prohibited.
d. When accessing email from a personally-owned device, Associates must ensure that the device is encrypted, has a strong password, and can be remotely wiped or disabled if it is lost or stolen.
e. Utilizing Wickr's communication systems for non-Wickr-related commercial use is prohibited.
f. Associates must not use third-party owned devices such as Internet kiosks, devices owned by friends or family, or hotel business center computers to access Wickr's communication systems unless utilizing VPN.
g. Wickr's communication systems must not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
   - Employees who receive any messages with this content from any Wickr employee must immediately report the matter to Human Resources.
h. Where technically feasible, all messages traversing Wickr's communication systems must be scanned for computer viruses, worms, or other executable items that could pose a threat to the security of the network. Messages identified as malicious must not be delivered to the recipient.
i. Reasonable and limited personal use of Wickr communication systems is permitted.
j. Associates do not have an expectation of privacy on all communication systems operated by Wickr.

[7] Personal email or messaging systems include services such as Gmail, Hotmail, Yahoo Mail, Outlook.com, etc.

k. Associates must report suspicious communications[8] to Information Security.

References

- SANS Email Policy
- Network Solutions Email Security Plan
- NIST SP 800-100 Information Security Handbook

[8] Suspicious communications may include those from unrecognized senders, requests for confidential information, and phishing emails

Document Management

Title: Secure Communication Standard			
Version	**Date**	**Author(s)**	**Comments**
1.0	11/24/2017	CH	Initial version

Appendix A: Approved Communication Tools

a. Wickr products. Approved for use with Public, Internal Use Only, Restricted, and Confidential information.

b. Corporate Email (Google Gmail). Approved for use with Public and Internal Use Only information. Approved for use with Restricted and Confidential information only if transmitted in the form of an appropriately encrypted attachment, the key to which must be transmitted in a manner suitable for Restricted or Confidential information.

c. Corporate internal social blogs and ticketing systems. Approved for use with Public, Internal Use Only, and Restricted information.

d. Corporate and personally owned fixed and mobile telephony systems and mobile SMS. Approved for use with Public and Internal Use Only information.

Appendix B: Additional Guidance

a. Use extreme caution when receiving unsolicited messages from unknown senders. Never click or open unsolicited links or attachments contained in suspicious communications as this could expose the companies computers and network to outside threats. If you believe such a message could be legitimate, establish trust by verifying the sender and obtaining additional context before engaging further.

b. Never respond to financial or other offers, no matter how legitimate they appear to be: legitimate companies do not request confidential information such as credit card or Social Security numbers by email; any sweepstakes or other offer that looks too good to be true should be ignored.

c. Never share your account password: as with any password, communications security information must be kept absolutely confidential.

d. Never forward an unsolicited message: you should not be reading it, much less forwarding it.

e. Never forward or initiate chain letters.

wickr

EPHEMERAL COMMUNICATION GUIDE

Part 3: Recommended Reading

Key Considerations for Adopting Ephemeral Communications Tools
- https://www.natlawreview.com/article/key-considerations-adopting-ephemeral-communications-tools

ABA Tech Report 2017
- https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

Instant Messaging for Posterity
- https://www.aei.org/publication/instant-messaging-for-posterity/

The Legal, Policy, and Technical Landscape Around Data Deletion
- https://cdt.org/insight/the-legal-policy-and-technical-landscape-around-data-deletion/

"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information
- https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1829&context=ublr

Preservation of Electronically Stored Information
- http://www.klgates.com/files/upload/DATG_Preservation_of_ESI.pdf

Managing Instant Communications in Modern Litigation
- http://www.trial.com/cle/materials/2012-ch/ahlin.pdf

New Strategies in Protecting Client Communications
- https://www.wickr.com/blog-archive/2017/10/4/new-strategies-in-protecting-client-communications

Attorney Client Privilege in the Digital Age
- https://www.wickr.com/blog-archive/2017/11/29/attorney-client-privilege-in-the-digital-age

Wickr GC Jennifer DeTrani on Ephemeral Messaging, Discovery, and the Waymo-Uber Suit
- http://blog.logikcull.com/wickr-gc-jennifer-detrani-on-ephemeral-messaging-discovery-and-the-waymo-uber-suit

Ponemon Institute, LLC, 2017 Cost of Data Breach Study; Global Analysis,
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Compliance, Governance & Oversight Council: Information Lifecycle Governance & Data Privacy

https://www.cgoc.com/?s=information+lifecycle+governance

Wickr Messaging Protocol

- https://www.wickr.com/wickr-messaging-protocol

Attacks on Group Messaging

- https://www.wickr.com/blog-archive/2018/1/11/attacks-on-group-messaging