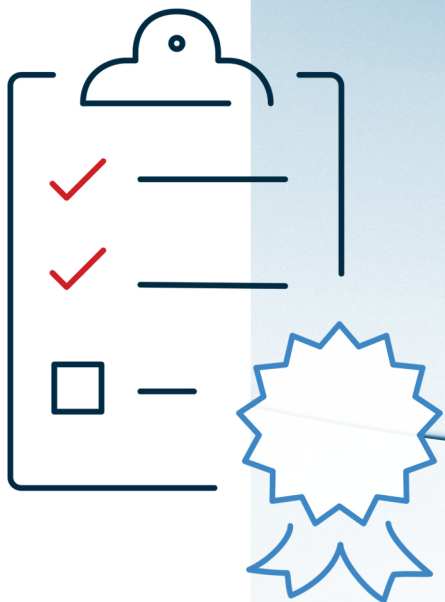
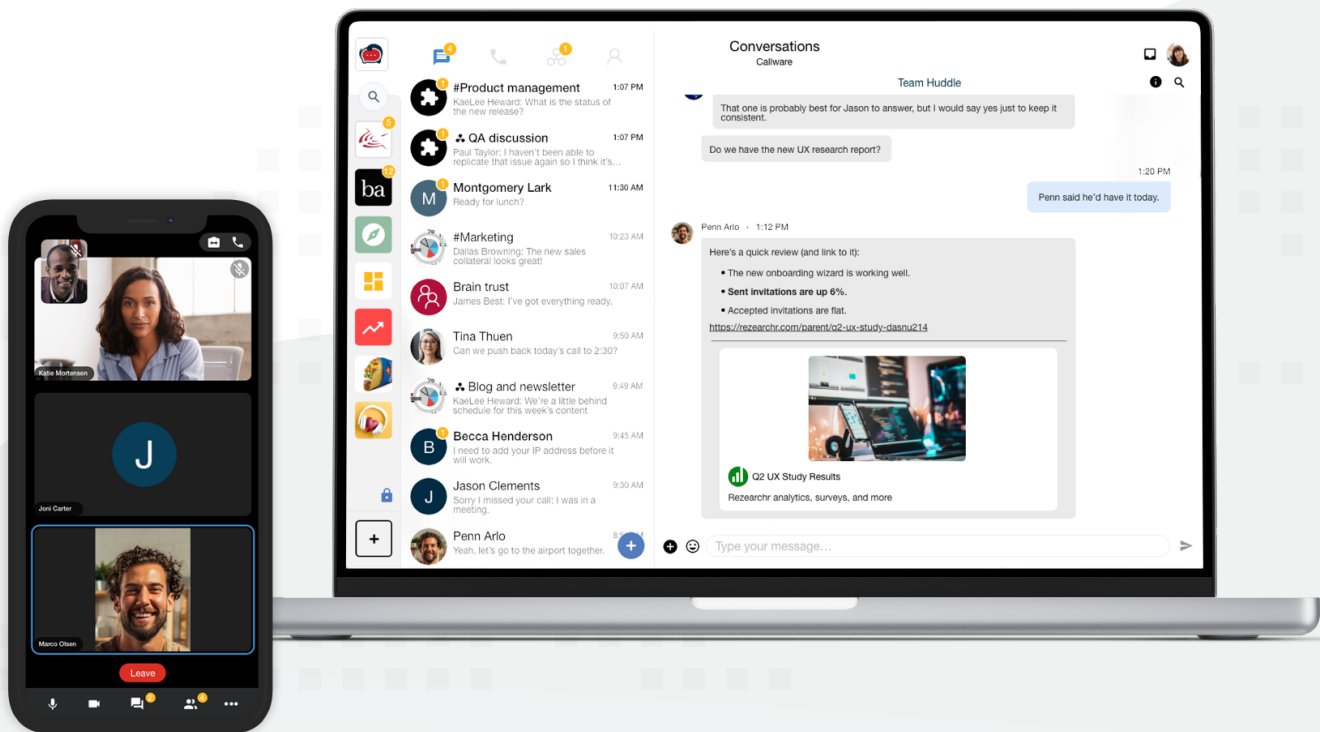


Communicate w/ Compliance



Whether you are a company with thousands of employees under intense regulatory scrutiny, an SMB with a solo IT manager, or have/are an MSP acting as CTO, your organization's data is under constant threat of exposure from careless negligence as well as external and internal bad actors. Staying compliant to regulatory requirements provides critical protections from such threats while reducing the potential for damages and any associated liability. By adopting a higher standard for data governance, organization's can advance compliance with secure communications using Lochbox.



Lochbox promotes the uninhibited exchange of sensitive information by making your communication data inaccessible to third-parties. More than just another messenger or meeting tool, Lochbox is a cybersecurity essential that gives organization's exclusive control over their encryption keys. Any conversation between employees, clients, or partners on Lochbox is under the custody and responsibility of the organization, allowing them to protect themselves from financial losses, license revocations, erosion of trust, and a damaged reputation that can come from a data breach and non-compliance.



WHAT IS COMPLIANCE?

In an economy that is ever more dependent on its use, data is both the fuel and byproduct of its function. Properly utilizing this resource can accelerate a business's growth while its neglect has the potential for irreparable harm. With incalculably high risks, businesses can't afford to not implement and follow a cybersecurity strategy. To be effective, strategies should include technologies, policies, and procedures designed to mitigate risk and reduce the threat vector or attack surface. Continuously following and adapting this strategy as needed is what compliance is all about.

Depending on an organization or individual's industry, they may have compliance policies required by associated agencies, laws, authorities, and even partners. Among the many reasons to be compliant with imposed privacy and security mandates, it's likely that avoiding legal repercussions are someone's primary (or sole) motivation. However, even when there is no impending threat of fines or lawsuits, establishing and observing effective policies is a judicious practice that safeguards the integrity of any business.

WHO NEEDS TO BE COMPLIANT?

Any industry that deals with sensitive and/or personally identifying information (PII) susceptible to misuse should be observing vetted privacy and security practices to protect operations, employees, vendors, and customers. Healthcare professionals and those working in financial services are examples of two industries with strict compliance standards dictating how communication data should be stored/transmitted, who can access it, and how those communications are conducted.

**MITIGATE RISK AND REDUCE
THE ATTACK SURFACE OR
THREAT VECTOR**

WHY DOES COMPLIANCE MATTER?

Cybersecurity best practices are instituted to protect all parties involved in the creation and management of sensitive data. Intellectual property, trade secrets, and PII are all at risk of abuse. Enforcing compliance standards helps safeguard this information from internal and external bad actors alike.

Explicit compliance reduces the risk of a data breach and the associated response and recovery costs, as well as the less-quantifiable costs such as reputation damage, business interruption, and loss of business. In the event that a data breach occurs, any cybersecurity insurance claims will be void without strict adherence to the required policies and standards.

HOW DOES LOCHBOX HELP WITH COMPLIANCE?

Regardless of industry or profession, communications are one of the most common sources of non-compliance. The pressure to communicate with customers and employees using their preferred communication method - i.e. whatever is most convenient - and not follow regulatory guidelines puts their sensitive information and your business at risk. Lochbox offers a unified solution that features everyone's favorite communication methods in one secure platform.

With Lochbox, clients and staff can now use texts, calls, and meetings to connect while having their conversations secured by end-to-end encryption with all content remaining encrypted at rest. Strict user controls ensure that client information is never exposed to other clients and only available to authorized and relevant personnel. Unsatisfied with simply meeting basic compliance standards, Lochbox utilizes on-prem and/or cloud servers that are independently managed by users to exceed some of the most strict data compliance requirements around.



HOW TO BE COMPLIANT

Creating a culture of compliance from the top down is essential for effective adoption and enforcement. Employees need to understand that compliance isn't about not sharing confidential information, it's about sharing it in the right way.

The following steps can help guide you through establishing the compliance standards that will benefit your organization most.

1 IDENTIFY THE TYPES OF DATA YOU WORK WITH AND THE REQUIREMENTS THAT MAY APPLY

Do you exchange payment or banking details, social security numbers, or record confidential information about your clients/customers? FINRA or HIPAA regulations likely apply.

2 APPOINT A CHIEF INFORMATION SECURITY OFFICER (CISO)

Anyone can be your company's CISO. Having technical knowledge helps, but their responsibilities are to develop, implement, and enforce security policies to protect critical data. Designating the responsibility to someone ensures that there is accountability within the organization.

3 CONDUCT RISK AND VULNERABILITY ASSESSMENTS

Determine where your organization's weaknesses are and how capable it is to independently manage those risks. If needed, outsourcing the areas where you are deficient will reduce internal burdens and better ensure compliance is met.

4 IMPLEMENT TECHNICAL CONTROLS BASED ON REQUIREMENTS AND RISK TOLERANCE

The proper storage and exchange of data is one example of areas that may require technical controls. Your organization's needs are unique and the solutions required to meet those needs may be equally unique.

5 IMPLEMENT POLICIES, PROCEDURES, AND PROCESS CONTROLS

Defining the required procedures and thoroughly educating employees on them is essential for effective compliance practices. The clearer the expectations and process the better.

6 REVIEW, TEST, ADAPT


Assessing the efficacy and efficiency of your cybersecurity plan takes time and practice. The policies and procedures may need adjusting and it's best to discover such issues to make the necessary changes before it's too late.


As important as it is to identify the standards and procedures relevant to your operations such steps are invalidated without a dedicated effort towards their observation and implementation. Lochbox simplifies and improves compliance, offering greater protection to your business, your reputation, and your customers.

Contact Us

 lochbox.app

 info@lochbox.app

 (801) 988-6800
(800) 225-5927

 8871 S Sandy Parkway, Suite 200
Sandy, UT 84070

