IPRO

WHITEPAPER

E-Collaboration Tools & Rules:

Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack & Other Videoconferencing & Meeting Tools

PART 1: Forming an E-Collaboration Policy Team and Conducting an Audit

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Nancy Flynn

Founder & Executive Director, The ePolicy Institute™

Author, The e-Policy Handbook, The ePolicy Toolkit, Social Media Rules, E-Mail Rules, Blog Rules, Instant Messaging Rules, Writing Effective E-Mail

Published October 2021

Sponsored by IPRO

PREFACE

IPRO and The ePolicy Institute™ have created this three-part whitepaper, **E-Collaboration Tools & Rules: Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack, and Other Videoconferencing & Meeting Tools** to help North American employers develop and implement compliant E-Collaboration Policy programs. Professionally written by the policy experts at the ePolicy Institute, **E-Collaboration Tools & Rules** is designed to help executives in all industries and professions—regulated and unregulated, large and small, public and private—minimize electronic risks, manage content and use, maintain records, and maximize legal and regulatory compliance.

Technology Evolves, But Policy Never Goes Out of Style

While technology continues to evolve—and its use in the workplace grows—one fact of strategic compliance management remains unchanged. Best practices always have—and always will—call for the establishment and enforcement of e-policies designed to manage employee behavior, mitigate employer risks, and maximize compliance with legal, regulatory, and organizational rules. Through the development and implementation of a strategic E-Collaboration Policy program, incorporating clear and comprehensive rules, companywide employee education, and proven-effective technology solutions, employers can reduce the likelihood of workplace lawsuits and regulatory audits, e-discovery disasters, security breaches, privacy violations, productivity drains, and other potentially costly mishaps.

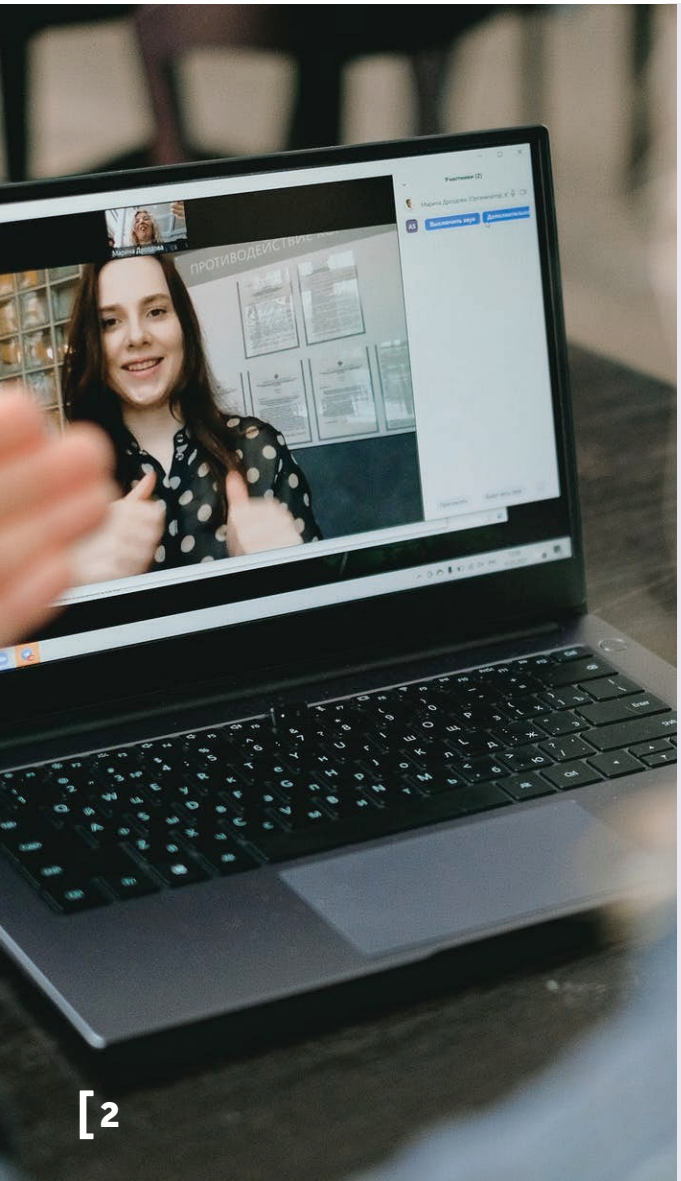
This three-part whitepaper provides a review of the risks inherent in real-time collaboration through instant messaging (IM), chat, videoconferencing, and virtual meetings. It then reveals how your organization can put a strategic E-Collaboration Policy program to work to help manage those risks. We encourage you to use this guide to help create your own E-Collaboration Policy program.

Contact Nancy@ePolicyInstitute.com

E-Collaboration Tools Are Here to Stay—Despite the Risks

Offering real-time communication through videoconferencing, IM, chat, and meetings, e-collaboration tools have established a solid foothold in the workplace.

When the pandemic stranded employees at home, Microsoft Teams exploded, growing from 20 million users in November 2019 to 145 million in April 2021.[i] Work-from-home (WFH) employees holding daily Zoom meetings grew to 300 million by April 2020.[ii] Slack saw a 25 percent uptick during a mere two-week period in March 2020.[iii] Unfortunately for employers, the COVID-19 collaboration boom has created a boatload of potentially costly legal, regulatory, and organizational challenges.



For North American employers—regulated and unregulated, large and small, public and private— mismanaged e-collaboration tools are more than a nuisance. They are a liability. Microsoft Teams, Zoom, Slack, and other e-collaboration platforms escalate legal, regulatory, records, e-discovery, privacy, security, and productivity risks. Fully 27 percent of organizations surveyed by Osterman Research report at least one employee has used Microsoft Teams to circumvent compliance requirements.[iv] Adding to the problem: Remote staff may be tempted to play fast and loose with language when Zooming from the kitchen table, increasing the likelihood of harassment, discrimination, and hostile work environment claims. In fact, according to Project Include, 45 percent of survey respondents have experienced harassment over chat during the pandemic, with another 41 percent reporting harassment during video meetings.[v]

Whether communicating internally with colleagues or externally with consumers and clients, risks soar when employees collaborate via videoconferencing, IM, chat, and virtual meetings.

Adopt the 3Es of E-Risk Management

To minimize risks, organizations must develop a strategic policy program to manage Microsoft Teams, Zoom, Slack, and other e-collaboration tools, supported by a Litigation Hold Policy and Deletion Schedule—and based on the 3Es of e-risk management:

Establish

effective E-Collaboration Policy & Procedures governing onsite and WFH staff.

Educate

employees about e-collaboration risks, rules, records, requirements, and roles.

Enforce

policies with discipline, education, and best-in-class technology solutions.

How to Get Started with an E-Collaboration Policy Program

Best Practice 1: Form an E-Collaboration Policy Team

The job of researching, writing, and implementing E-Collaboration Policy is too big for one person to manage. Adhere to best practices and form a team to oversee the development and administration of your E-Collaboration Policy program. The size and makeup of your policy team will depend on the nature of your business, exposure to online risks, and availability of financial and human resources. **The ideal team will take shape as follows:**

• **Senior Executive or Policy Champion:** To help convince employees that the organization is serious about e-collaboration compliance and risk management, recruit a senior executive (the more senior the better) to serve as the champion, or public face, of E-Collaboration Policy.

• **Legal:** Unfortunately, when it comes to the adoption of Microsoft Teams, only 50 percent of organizations surveyed view Legal as a key decision maker.[vi] This is a dangerous oversight. Do not roll out E-Collaboration Policy until it's been vetted by Legal. Rely on Legal to draft Litigation Hold Policy. Trust Legal to ensure all federal/state laws and industry/government regulations are addressed and employees' rights are protected. The participation of an experienced lawyer on your E-Collaboration Policy team will signal the organization's commitment to compliance. In the event of a lawsuit, Legal's contribution will help demonstrate that you've done your due diligence and are serious about managing e-collaboration risks, records, content, and use.

• **IT:** On the other hand, 85 percent of surveyed businesses rank IT as very or extremely influential in the decision to embrace Microsoft Teams.[vii] That's good news. IT should play a lead role on the E-Collaboration Policy team. IT's task is to assess and address privacy concerns, security vulnerabilities, and technology solutions—including the decision to manage records and risks either with native or third-party archiving, data protection, and e-discovery tools.

• **Records Management/Information Governance:** Just like email and social media, the content created by Zoom, Slack, Microsoft Teams, and other e-collaboration tools can create business records that must be managed and maintained for business, legal, and regulatory reasons. Failure to preserve, protect, and produce records in response to subpoenas, public records requests, or regulatory audits can land your organization in hot water. Put Records/Information Governance on the team. Assign them the task of reviewing and recommending Records Retention Policy, records lifecycles, and deletion schedules.

• **Human Resources (HR):** Typically charged with enforcing rules and addressing violations, HR is integral to the E-Collaboration Policy team. Grant HR a role in every aspect of your compliance management program, from writing policy to educating employees to disciplining rule breakers.

• **Training:** You cannot expect an untrained workforce to comply with policy. Formal, ongoing education is crucial to the success of your E-Collaboration Policy program. Demonstrate your commitment to compliance, communication, and civility by including Training on the team—and making workforce education a priority.

• **Public Relations (PR):** In the event of an electronic disaster, PR will be responsible for keeping employees, the media, customers, and investors informed, while squelching rumors and burnishing your brand. Hope for the best, but plan for the worst by incorporating a crisis communications plan into your E-Collaboration Policy program.

Best Practice 2:

Conduct a 7-Step E-Collaboration Policy Audit

After you've established a policy team, the new group will need to conduct an E-Collaboration Policy audit. This research will help determine the risks, rules, regulations, records, roles, and requirements to be addressed.

Audit Step 1. Review Risks & Policy Solutions

All electronic business communications tools—from email to Zoom—share legal, regulatory, and organizational challenges. The solution: Apply best practices-based policies to minimize risks, manage behavior, and maximize compliance. For example:

Records Risk: Just as email creates business records that must be preserved, protected, produced, and purged, so too does Microsoft Teams.
Policy Solution: Couple E-Collaboration Policy with Records Retention Policy and Litigation Hold Policy to manage and maintain business records.

Privacy Risk: Just as untrained employees might accidentally expose confidential company information and private consumer data via email, so too might rogue employees intentionally spill the beans via unauthorized Zoom screen sharing.
Policy Solution: Incorporate content and usage rules into your E-Collaboration Policy to safeguard privacy and shore up security.

Evidentiary Risk: Just as you can delete email, so too can you delete Slack messages. In both cases, deleted messages may return to haunt you in the form of evidence if they originated—and continue to exist—outside your organization and its control.
Policy Solution: Combine E-Collaboration Policy with Records Retention Policy and Litigation Hold Policy to limit evidentiary risks.

E-Discovery Risk: Just as email e-discovery slipups can lead to six- and seven- figure court sanctions, legal settlements, and jury awards, so too can your failure to promptly locate and properly turn over subpoenaed Microsoft Teams and Zoom records.
Solution: Match E-Collaboration Policy with Records Retention Policy and Litigation Hold Policy to deflect e-discovery disasters.

Litigation Risk: Just as inappropriate email can trigger workplace lawsuits and provide smoking-gun evidence in litigation, so too can unlawful and objectionable videoconference, webinar, IM, chat, and meeting content.
Policy Solution: Support E-Collaboration Policy with comprehensive training and best-of-breed technology to protect your organization's assets, reputation, and future.

"Since the start of the pandemic, employees have felt as if online environments are the Wild West, where traditional rules do not apply." [viii]

Audit Step 2. Research All Applicable Laws

Research all the legal risks and rules facing your organization. That includes laws governing electronic use, content, monitoring, e-discovery, privacy, security, and other concerns. Be sure to review the laws of every jurisdiction (international, federal, state, local) in which you operate, employ workers, serve customers, litigate claims, or otherwise have a business presence.

In the U.S., for example, employers in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands must comply with data breach notification laws, designed to protect consumers and penalize businesses that fail to secure personally identifiable information (PII) and financial privacy.

If you operate facilities or conduct business in the European Union, you must adhere to the General Data Protection Regulation (GDPR), which allows citizens/residents to access/delete personal electronic information held by companies.

Once your comprehensive legal review is complete, determine exactly what your organization needs to do—from the standpoint of E-Collaboration Policy, employee training, and third-party technology solutions—to achieve 100 percent legal compliance on the international, federal, state, and local levels. Fail to complete this step, and you may find yourself on the wrong side of a workplace lawsuit triggered by defamatory, discriminatory, harassing, or otherwise illegal or inappropriate content.

Audit Step 3. Review Regulatory Rules

Organizations operating in the financial sector, healthcare arena, and other highly regulated industries must know and adhere to all regulatory guidelines governing the business. The Health Insurance Portability and Accountability Act (HIPAA), for example, requires healthcare entities to protect patients' electronic protected health information (EPHI).

Three of the myriad regulatory bodies and regulations impacting the financial industry: **(1) Financial Industry Regulatory Authority (FINRA**), which requires security firms and broker dealers to safeguard the storage and sharing of investors' confidential information; (**2) Gramm-Leach-Bliley Act (GLBA)**, which obligates financial institutions to protect the nonpublic personal information (NPI) of customers and consumers; and **(3) New York Stock Exchange (NYSE),** which requires listed companies to adhere to the exchange's electronic record retention and content guidelines, including protecting confidential business records and personal customer information that is stored and transmitted electronically.

Regulatory rules apply to e-collaboration and videoconferencing platforms, as well as email and social media. Your goal is to determine exactly what your organization needs to do—in terms of policy, training, and technology—to adhere to all the industry and government regulations impacting your business. Skip this step, and it's possible that intrusive messages about patients or premature communications about financials could spark regulatory investigations and fines.

"Consider sensitivity of data before exposing it via screen share or uploading it during video conferences. Do not discuss information that you would not discuss over regular telephone lines." [ix]

Audit Step 4. Research Data Security Risks

The workplace use of e-collaboration and videoconferencing platforms has grown so rapidly that many organizations have yet to implement much-needed security precautions—or may be unaware of the security vulnerabilities posed by Microsoft Teams, Zoom, Slack, and similar tools. Appoint IT the task of researching security risks and ensuring employees can connect and communicate safely from the office or home. Review and update rules governing security settings, passwords, Wi-Fi networks, encryption settings, privacy settings, security updates/patches, and other tools designed to keep sensitive information safe from unauthorized internal exposure and unwanted attacks by malicious parties including zoombombers who show up—uninvited—to videoconferences.

Audit Step 5. Assess the Ways in Which Your Organization Uses E-Collaboration Tools

Ask the 5Ws: **Who** is using **what** e-collaboration platform, **when, why,** and **how?** In light of the fact that IM traffic increases 52 percent between 6 p.m. and midnight,[x] be sure to explore employees' after-hours activity, as well as 9-to-5 use. Armed with answers to the 5Ws, move on to audit step six.

Audit Step 6. Decide What Tools to Authorize for Business Use

Microsoft Teams, Zoom, and Slack are just three of many e-collaboration tools available for business use. Four of 10 organizations surveyed report using Microsoft Teams along with three or more other collaboration tools.[xi] Based on your audit results and the expertise of IT, Legal, Records Management, and other policy team members, decide which tool (or tools) to authorize for business communications. Use E-Collaboration Policy to notify employees that the use of any other tools is strictly prohibited—at the office, home, or elsewhere.

Audit Step 7. Review Existing Electronic & HR Policies

In light of e-collaboration risks and rules, now may be a good time to review and update related electronic and HR policies and guidelines. With collaboration and videoconferencing in mind, take a look at your organization's Mobile Device Policy; Email Policy; Social Media Policy; Web Policy; Security Policy; Privacy Policy; Monitoring Policy; Harassment & Discrimination Policy; Diversity & Inclusion Policy; Confidential & Sensitive Information Policy; Code of Conduct; Ethics Rules; Netiquette Rules; Videoconference Dress Code and Virtual Background Guide; and so on.

Be sure to cross-reference policies as appropriate. For example, use E-Collaboration Policy to inform employees that they must adhere to the company's Harassment & Discrimination Policy and Code of Conduct when videoconferencing. Use Mobile Device Policy to explain that e-collaboration rules apply 24/7/365, regardless of the tool—iPhone, tablet, laptop—used to engage in Microsoft Teams meetings or Zoom webinars. Provide links, so users quickly can access, read, and comply with all guidelines.

Conclusion: Collaboration Compliance Is as Easy as 1,2,3

This whitepaper—E-Collaboration Tools & Rules: Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack, and Other Videoconferencing & Meeting Tools —is divided into three parts:

Part 1: Forming an E-Collaboration Policy Team and Conducting an Audit.
Part 2: Getting to Work on Policy Rules.
Part 3: Technology and Education.

We encourage you to download and use this three-part series to help create your own E-Collaboration Policy program.

IPRO

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Seek Competent Legal Counsel

E-Collaboration Tools & Rules: Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack, and Other Videoconferencing & Meeting Tools is a general best-practices guide and is intended for informational purposes only. This material is provided with the understanding that neither the ePolicy Institute nor IPRO is rendering legal or regulatory guidance. The author did not and could not contemplate every issue, challenge, or situation that may arise when using e-collaboration tools. Some organizations may be required to comply with different or additional laws, regulations, rules, and procedures from those addressed in this whitepaper. No reliance should be placed on this whitepaper without the advice of experienced legal counsel and other competent professionals including regulatory, records management, IT, security, privacy, and HR experts. Your organization's E-Collaboration Policy (and all electronic policies and procedures for that matter) should be developed with the assistance of a capable attorney.

About The ePolicy Institute

The world's leading e-policy writing, training, and consulting firm, The ePolicy Institute helps employers cut legal and regulatory risks and boost compliance through best practices-based electronic policies and employee training programs. From Alabama to Abu Dhabi, employers rely on the ePolicy Institute to help ensure compliance and reduce risks through the implementation of e-policies governing email, social media, mobile devices, e-collaboration platforms, web, and other electronic business communications tools. An industry pioneer, Founder Nancy Flynn is the author of **The e-Policy Handbook,** the first book to address electronic policies and procedures in the workplace. Her other titles include **The ePolicy Toolkit, The Social Media Handbook,** and **Writing Effective E-Mail.** Trusted for her know-how and integrity, Nancy Flynn is a go-to media source who serves as an expert witness in policy-related litigation. The ePolicy Institute. Keeping you in business and out of court since 1998. Visit **ePolicyInstitute.com** to learn more.

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

IPRO

About IPRO

IPRO is reinventing the way organizations interact with their data. By transforming the electronic discovery reference model (EDRM) and thinking "upstream," we bring insight far earlier in the eDiscovery process, enabling teams inside and outside your organization to collaborate transparently at any stage before data is even collected. By thinking about and interacting with your data differently, you will eliminate waste and reduce risk. We combine best-in-class governance and eDiscovery software with predictive analytics to give corporations, government agencies, law firms, and legal partners the most open and effective solution to data challenges. We bring you this power with an obsession on time-to-value and your success. Visit **IPRO.com** to learn more.

Contact Nancy@ePolicyInstitute.com

i Microsoft, "Microsoft Fiscal Year 2021 Third Quarter Earnings Conference Call," April 27, 2021. https://www.microsoft.com/en-us/Investor/events/FY-2021/earnings-fy-2021-q3.aspx.

ii Zoom Blog, "90-Day Security Plan Progress Report: April 22, 2020." https://blog.zoom.us/90-day-security-plan-progress-report-april-22/.

iii Slack, "Slack CEO Stewart Butterfield Shares Updated Business Metrics During Tweetstorm on Impact of COVID-19," March 26, 2020. https://investor.slackhq.com/news/news-details/2020/Slack-CEO-Stewart-Butterfield-Shares-Updated-Business-Metrics-During-Tweetstorm-on-Impact-of-COVID-19/default.aspx.

iv Osterman Research White Paper, sponsored by IPRO, "Archiving and Data Protection with Microsoft Teams," May 2021. https://ipro.com/resources/white-papers/archiving-and-data-protection-with-microsoft-teams/.

v Project Include, "Remote Work Since Covid-19 Is Exacerbating Harm: What Companies Need To Know and Do," March 2021. https://projectinclude.org/assets/pdf/Project_Include_Harassment_Report_0321_R8.pdf.

vi Osterman Research White Paper, sponsored by IPRO, "Archiving and Data Protection with Microsoft Teams," May 2021. https://ipro.com/resources/white-papers/archiving-and-data-protection-with-microsoft-teams/.

vii Ibid.

viii Leah Fessler quoting Jennifer Brown, "Workplace Harassment in the Age of Remote Work," *The New York Times*, June 8, 2021. https://www.nytimes.com/2021/06/08/us/workplace-harassment-remote-work.html?

ix Cybersecurity and Infrastructure Security Agency (CISA), "Guidance for Securing Video Conferencing." https://www.cisa.gov/publication/guidance-securing-video-conferencing.

x Chris Matyszczyk, "Microsoft Told Employees to Work from Home. One Consequence Was Brutal," *Technically Incorrect,*" July 26,2020. https://www.zdnet.com/article/microsoft-told-employees-to-work-from-home-one-consequence-was-brutal/.

xi Osterman Research White Paper, sponsored by IPRO, "Archiving and Data Protection with Microsoft Teams," May 2021. https://ipro.com/resources/white-papers/archiving-and-data-protection-with-microsoft-teams/.