2021 Privacy & Security Resource Guidebook

Alliant

PRIVACY & SECURITY:
NOW MORE THAN EVER

Learning from past events and experiences is quintessential to staying secure, but the central element to privacy and security is “right now.” What are you doing to ensure that you’re always on guard and making wise decisions to avoid a potential breach? What you do right here, right now, could dramatically alter the future, as we live in a highly connected, highly fraught informational landscape.

This resource is an essential tool to help you practice wise privacy and security habits at any time, in any place. Read it, save it, and consult it regularly to ensure you’re on top of your game!

Ahead of the Game

Privacy and security never sleeps. Threats abound, and they change by the day with new vulnerabilities surfacing at a moment's notice. Alliant is doing its part to ensure that our company is secure now, and for the long haul. Here are some of the measures we are taking to stay ahead of the game to safeguard our employees, our clients, and our organization:

Vendor management: We ask our vendors to complete security questionnaires and ensure that vendor IT security practices are aligned with Alliant's protocols and comply with our legal, regulatory, and contractual obligations.

Audits: We conduct annual security audits that focus on various aspects of the company, ranging from AlliantConnect to our overall technology infrastructure. We also conduct a HITRUST audit, which evaluates privacy and security practices within our industry and provides continuous benchmarks for improvement.

System security and monitoring: We've contracted with some of the best privacy and security vendors in the business to ensure our systems are safe and secure. One example of this is CrowdStrike, a 24/7 service that monitors our networks, servers, and systems to identify any irregular activity. We also conduct penetration testing and email phishing tests to evaluate our readiness should an attempted hack occur.

In addition to these ongoing initiatives, we are continuously monitoring trends and changes in the privacy and security landscape to ensure we are up to speed on the newest threats and vulnerabilities and are ready to respond at a moment's notice.

Keep Your Outlook Spic and Span

Email continues to be a hot spot for privacy and security threats. Just one wrong click and a hacker could gain access to every email in your system and cause havoc by accessing critical company, client, and personal data.

Keep your Outlook spic and span with these easy-to-use tools to ensure the wrong person doesn't get their hands on critical information:

- **Shortcuts** for fast and easy categorization and deletion of emails—clean up your Outlook inbox in one easy step
- A **Rules** function that automatically moves sensitive data to a secure location
- The ability to **group** multiple emails on the same topic
- A large **list** of options for sorting to help you locate, delete, or move sensitive emails
- **Conversation Cleanup**, which evaluates the content of messages so duplicates can be removed

Alliant has created a detailed guide that will take you step-by-step through all of these critical functions.

Outlook is a part of everything we do on the job, and keeping it clean is a crucial step to ensuring your security, and that of Alliant.

Let's (Keep Talking) About Phishing

Phishing is a long-used form of deception that uses what appears to be a legitimate email or website to mine for personal information. And while this practice is not new, it grows more sophisticated by the day. From spyware to ransomware to invoice fraud, hackers are constantly looking for new and innovative ways to deceive and defraud.

Oftentimes, you are the last line of defense. Here are some proven tactics you can use to stop phishing in its tracks.

- **Question everything** and closely analyze any request for sensitive data or funds. Remember: in addition to emails, some of the most brazen hackers will even make direct phone calls posing as a reliable source.
- **Confirm all requests** by direct and verbal communication.
- **Look closely** at the email address and compare it to prior emails to confirm it is not engineered to look like the real deal. In many cases, the company domain may be slightly misspelled (for example, John.Doe@aliant.com).
- **Never open** a document or click on a link in an email that you cannot confirm as legitimate, and never provide personal information, logins, or passwords.
- **Report it**; if you think you have received a phishing email, contact the Help Desk at helpdesk@alliant.com or call (619) 849-3911. And if you happened to accidentally click on the wrong link or open the wrong document, it is imperative you report that, too.

Monitor. Confirm. Report. Those are the three foundational elements of privacy and security, and they are your ultimate defense in the ongoing fight against phishing.

The Rise of Invoice Fraud

Think twice about that invoice you just received. Cases of invoice fraud are rising worldwide, and scammers are finding new and innovative ways to create fake invoices and convince unknowing targets to pay up.

Picture this: You receive an email or phone call from what appears to be a client or vendor. They ask you to wire the funds to a different location and provide you with new wire transfer information. Although this seems like standard operating procedure, it is actually a brazen attempt to defraud the company out of what could be millions of dollars.

Here's how you can stop them:

Examine the email address. Is it an official company email, or is it manufactured to look like the real deal? Also, look out for poor grammar and misspellings.

Review the invoice. Is it on official company letterhead? And if so, does anything look off? In many cases, hackers will cut and paste logos and headers from outside sources to create fake invoices.

Call your client or vendor directly and verify that the request is legitimate.

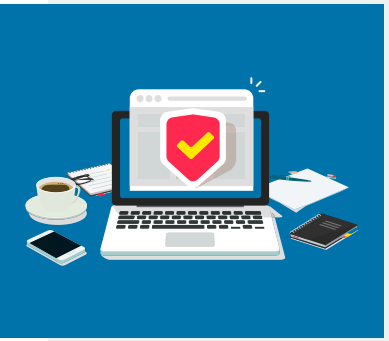
Forward the email in question to all of your contacts with the client or vendor to ensure they are aware of this request. This should be done in addition to a phone call.

Invoice fraud is one of the fastest-growing and most urgent privacy and security issues facing our industry today. Examine all invoices carefully and, as always, question everything!

Safe at Home

Working from home is the order of the day. The virtual office is everywhere, from your home to your car to your local coffee shop. Although this means greater convenience and mobility for the workforce, privacy and security threats abound.

Remember, even when you're not in your physical office, you are still vulnerable. Take the following key measures to practice privacy and security from any location:



Secure your laptop: Done working for the day? Lock your laptop away in a secure location. And if you're on the road, make sure it is with you at all times or hidden away in your trunk.

Secure your physical space: Never leave confidential information out in the open, particularly on your printer. Shred all documents in question and keep your home office clean and organized.

Be private in public: If you are working remotely in a public space, only use secure, password-protected networks. Never leave your laptop unattended and be careful not to have confidential phone conversations in places where you could be heard.

Proceed carefully: User error is the #1 cause of data breaches. Every move you make could potentially expose confidential information. Be diligent, and when sending emails, be sure you are sending them to the right recipient and not just the first name that auto-fills in the "To…" field.

Okta is your friend: Okta must be installed on all your devices. You need it for secure user authentication into all of our company apps, and it is required for your company Zoom.

Alliant

Privacy & Security Resource Guidebook

Privacy & Security Team

We're here to help! Alliant has a team of dedicated Privacy & Security Officers working hard to keep our company safe and secure:

Jennifer Baumann, General Counsel

Kristine Blanco, Privacy Officer, Data Privacy Officer

Diana Kiehl, Chief Administrative Officer

Kyra Kono, Privacy Deputy

Mike Popp, Security Deputy

Jacob Rubin, Privacy Deputy

Steve Sampiere, Chief Information Officer

Ryan Skadberg, Security Officer

Dustin Wolverton, Security Communicator

Scott Yates, Security Deputy