ombuds.org

Cybersecurity Best Practices for Ombuds

Updated January 24, 2022

Why should ombuds worry about cybersecurity?

As we move more of our lives online, especially in the wake of the global pandemic, cybersecurity is growing in importance. The measures we have taken in the past to protect the privacy of our visitors are no longer adequate when visitors are reaching out to us through online channels. Every email, text message, and video chat can generate sensitive information, and it is your responsibility to ensure that all information shared with your office is appropriately managed and protected.

If your office is a victim of unauthorized access, it may cause harm to your visitors, inflict reputational damage to your program, and potentially trigger regulatory sanctions. What's more, cyberattacks are growing in frequency and complexity; your cybersecurity practices may be at a high standard today, but if you don't continue to update them you may be vulnerable to new attacks tomorrow.

In order to help you mitigate the risk to your office of cyber breaches, we have prepared this list of best practices that detail some simple steps you can take to protect your team and your visitors:

Before:

1. Draft cybersecurity protocols and policies for your office
2. Hold staff trainings on cybersecurity best practices
3. Designate a cybersecurity contact person on your team
4. Explore insurance to cover potential damages
5. Utilize software platforms that ensure data security (e.g. ISO 27001 compliant)
6. Understand your compliance obligations to relevant laws and regulations
7. Tailor access rights to all data, so you know who has access to what
8. Update and patch your software and hardware
9. Secure your local software, hardware, and network

During:

1. Make cybersecurity policies, responsibilities, and protocols explicit
2. Update your policies and procedures based on changing circumstances and user feedback
3. Maintain access control rules (e.g. monthly change of password, limited time of access to documents, automated logout from shared platforms)
4. Monitor vulnerabilities by setting up instant alerts for unauthorized access
5. Stay alert for red flags (e.g. cloned emails, suspicious attachments/links)
6. Report any attack or intrusion immediately
7. Keep track of where your data goes throughout all interactions with visitors
8. Conduct periodic data backups

9. Encrypt sensitive information, both in transit (over the internet) and at rest (on your drive)
10. Avoid using free service providers (for email, data transfer, antivirus scanning)
11. Select settings that protect the security of your video conferencing sessions
12. Limit copies to portable devices (e.g. USBs, mobile phones, external drives)
13. Control all access to hard copies of data
14. Use privacy screens and webcam covers

After:

1. Return or destroy any physical documents with sensitive data
2. Get a final security report from your software platform confirming that personally identifiable information (PII) has been deleted/anonymized
3. Encrypt or delete any archived information on your hard drives

Protecting your online identity:

1. Create a confirmed profile on social media (so no one can pretend to be you)
2. Disclose close relationships reflected on social media to avoid challenges to your impartiality
3. Audit and prune your social networks
4. Select safe private messaging tools
5. Use non-public chat integrated into secure online platforms whenever possible
6. Think before you click to avoid phishing attacks through social media

Be Alert

Never be off guard. Every internet interaction creates an opportunity for a cyber-threat. We may do things automatically without much thought, such as clicking on emails that seem to be from the visitor (but actually have a slightly changed address), or clicking non-verified links to download files, that may then compromise your security via a phishing attack. If you have any doubts, make a phone call or reach out to the sender by other means for a second verification before you click.

Work as a Team

Everyone can be the weak link. Anyone who uses the internet can trigger an exposure that can impact all others involved. A cybersecure office is thus highly dependent on excellent teamwork in which everyone takes precautions, and adequate guidance or training to all involved is essential.

Be Proactive

Do not wait for the risk to materialize before taking measures. You should consider taking precautionary measures before a risk becomes imminent. Being prepared requires frequent checks and updates. Merely taking measures at the beginning will not adequately eliminate the risks faced throughout; routine checks up shall also be made throughout the entire process.

Respond Quickly

Time is of the essence. Once an exposure happens, the longer it takes to tackle it, the more costly it will be to fix the damage. Cybersecurity requires teams to prepare in advance, and protocols for interventions should have a pre-established list of measures to mitigate potential damages.