2023 New York Statewide Civil Legal Aid Technology Conference

3C Cybersecurity: Practical Considerations and Best Practices
Wednesday, April 19, 2023
2:00 PM – 2:50 PM
Live Virtual Presentation
CLE Credits: 1.0 Cybersecurity, Data and Privacy - General

CLE RESOURCES

Free and Low-Cost Tools, Government Resources, Funding Opportunities

Sample Employee Internet Usage Policy

Sample Email Usage Policy Template

Sample Social Media Policy for Employees

PRESENTERS

Moderator: John Greiner, President, Just-Tech

Panelists:

Christine Sisario, Chief Information Officer, NYS Unified Court System

Courtney Kanopka, Deputy Chief Information Security Officer/SOC Manager for the NYS Court Unified Court System, Division of Technology and Court Research

Free and Low-Cost Tools, Government Resources, Funding Opportunities

CYBERSECURITY: PRACTICAL CONSIDERATIONS AND BEST PRACTICES

FREE AND LOW-COST TOOLS, GOVERNMENT RESOURCES, FUNDING OPPORTUNITIES

SANS – Free Cyber Security Training - https://www.sans.org/cyberaces/

- Launched in 1989 as a cooperative for information security thought leadership, it is SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

KnowBe4 – Security Awareness Training Resources - https://www.knowbe4.com/resources

- Forrester Research has named KnowBe4 a Leader in Forrester Wave for Security Awareness and Training Solutions for several years in a row. KnowBe4 received the highest scores possible in 17 of the 23 evaluation criteria, including learner content and go-to-market approach.

CrowdStrike – Free 15-day trial - CrowdStrike: Stop breaches. Drive business.

- Market leading next generation anti-virus to stop malware with integrated threat intelligence and immediate response. CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of enterprise risk – endpoints and cloud workloads, identity, and data – to keep customers ahead of today's adversaries and stop breaches.

MS-ISAC - Leading the global community to secure our ever-changing connected world - https://www.cisecurity.org/isac

- Center for Internet Security (CIS) is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CISA – America's Cyber Defense Agency - Home Page | CISA

- The operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.

HaveIBeenPwned.com

- A free resource for anyone to quickly assess if they may have been put at risk due to their email address or phone number being compromised or "pwned" in a data breach.

Virustotal.com

- A free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content. Our goal is to make the internet a safer place through collaboration between members of the antivirus industry, researchers, and end users of all kinds.

Cyber Grant Funding Opportunities:

NYS Division of Homeland Security and Emergency Services- Grant opportunities
https://www.dhses.ny.gov/nonprofit-programs

Federal Emergency Management Agency - Grant opportunities
https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

Governor Hochul Announces Expansion of State’s Major Investments in Cybersecurity Initiatives -
https://www.governor.ny.gov/news/governor-hochul-announces-expansion-states-major-investments-cybersecurity-initiatives

Sample Employee Internet Usage Policy

Sample Employee Internet Usage Policy

This **Employee Internet Usage Policy** is ready to be tailored for your company's needs and should be considered a starting point for setting up your policies regarding computer usage for employees. May also be called **Employee Internet Policy**, **Company Internet Policy** or **Computer Usage Policy**.

Policy brief & purpose

Our employee internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

Scope

This employee internet usage policy applies to all our employees, contractors, volunteers and partners who access our network and computers.

Employee internet usage policy elements

What is appropriate employee internet usage?

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate employee internet usage?

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.

- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask [*their supervisor/ IT manager/ etc.*]

Our company may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Company-issued equipment

We expect our employees to respect and protect our company's equipment. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

Email

Our employees can use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

Our company has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Disclaimer: This employee internet usage policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.

Sample Email Usage Policy Template

Sample email usage policy template

This corporate email usage policy template is ready to be tailored to your company's needs and should be considered a starting point for setting up your employment policies.

Policy brief & purpose

Our corporate email usage policy helps employees use their company email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their corporate email accounts.

Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

Scope

This policy applies to all employees, vendors and partners who are assigned (or given access to) a corporate email. This email may be assigned to an individual (e.g. employeename@companydomain) or department (e.g. hr@companydomain.com.)

Policy elements

Corporate emails are powerful tools that help employees in their jobs. Employees should use their company email primarily for work-related purposes. However, we want to provide employees with some freedom to use their emails for personal reasons.

We will define what constitutes appropriate and inappropriate use.

Inappropriate use of company email

Our employees represent our company whenever they use their corporate email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Our company has the right to monitor and archive corporate emails.

Appropriate use of corporate email

Employees are allowed to use their corporate email for work-related purposes without limitations. For example, employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.

- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Personal use

Employees are allowed to use their corporate email for some personal reasons. For example, employees can use their corporate email to:

- Register for classes or meetups.
- Send emails to friends and family as long as they don't spam or disclose confidential information.
- Download ebooks, guides and other content for their personal use as long as it is safe and appropriate.

Employees must adhere to this policy at all times, in addition to our confidentiality and data protection guidelines.

Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask our [*Security Specialists*.]

We remind our employees to keep their anti-malware programs updated.

Email signature

We encourage employees to create an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here's a template of an acceptable email signature:

[Employee Name]

[Employee Title], [Company Name with link]

[Phone number] | *[Company Address]*

Employees may also include professional images, company logos and work-related videos and links in email signatures. If they are unsure how to do so, they can ask for help from our Office Manager or their supervisor.

Disciplinary action

Employees who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

- Using a corporate email address to send confidential data without authorization.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a corporate email for an illegal activity.

Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.

Sample Social Media Policy for Employees

Sample social media policy for employees

This sample **Employee Social Media Policy** is a good starting point for fleshing out your own policy for use of social media in the workplace by your employees.

What is a corporate social media policy?

Most of your employees are likely to use one or more social platforms. Whatever they post on their personal accounts can be a potential risk for your company (e.g. if they share sensitive information). And, more importantly, using social media at work can affect productivity and focus. This is one of the reasons you need a company social media policy – to address limitations on what employees can post and to potentially place restrictions on social media use inside the workplace.

The other reason is your own social media profile; as an organization, you'll want to have a consistent voice on your social media and want to avoid posting potentially risky statements or information. A social media policy for employees can give them the instructions they need to know how to handle corporate accounts.

How restrictive should my company social media policy be?

Your employees own their social media profiles, so what they post there can't be restricted by your organization. You can, however, provide them with reasonable guidelines about what they shouldn't post about (e.g. confidential data) and provide any potential disciplinary actions if their posts affect your company's image (e.g. hate speech). As far as your own company's social media accounts are concerned, you're entitled to set the rules of posting.

How do I distribute it?

Your social media policy should be part of your employee handbook or live inside your policy database (e.g. in your HRIS). Make sure all employees have read it, especially those in your social media team.

Of course, remember that this policy is a living document – this is because the social media landscape changes often, new rules and regulations about privacy are introduced and trends can also play a part (e.g. the #metoo movement). Make sure you keep up-to-date with changes and think about whether your company social media policy might need some revamping.

Here's a simple social media policy template to get you started with the essentials:

Policy brief & purpose

Our **social media company policy** provides a framework for using social media. Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether you're handling a corporate account or using one of your own, you should remain productive and avoid damaging our organization in any way. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace.

Scope

We expect all our employees to follow this policy.

Also, by “social media”, we refer to a variety of online communities like blogs, social networks, chat rooms and forums – not just platforms like Facebook or Twitter.

This policy is built around two different elements: one, using personal social media at work and two, representing our company through social media.

Policy elements

Using personal social media

We *[allow]* our employees to access their personal accounts at work. But, we expect you to act responsibly and ensure your productivity isn't affected.

Whether you’re using your accounts for business or personal purposes, you may easily get sidetracked by the vast amount of available content. So, please restrict your use to a few minutes per work day.

We ask you to be careful when posting on social media, too. We can’t restrict what you post there, but we expect you to adhere to our confidentiality policies at all times. We also caution you to avoid violating our anti-harassment policies or posting something that might make your collaboration with your colleagues more difficult (e.g. hate speech against groups where colleagues belong to). In general, please:

We advise our employees to:

- **Ensure others know that your personal account or statements don’t represent our company.** You shouldn’t state or imply that your personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as “opinions are my own” to avoid misunderstandings.
- **Avoid sharing intellectual property** like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- **Avoid any defamatory, offensive or derogatory content.** It may be considered as a violation of our company’s anti-harassment policy, if directed towards colleagues, clients or partners.

Representing our company

Some employees represent our company by handling corporate social media accounts or speak on our company’s behalf. When you’re sitting behind a corporate social media account, we expect you to act carefully and responsibly to protect our company’s image and reputation. You should:

- **Be respectful, polite and patient,** when engaging in conversations on our company's behalf. You should be extra careful when making declarations or promises towards customers and stakeholders.
- **Avoid speaking on matters outside your field of expertise** when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else’s responsibility.

- **Follow our confidentiality policy and data protection policy** and observe laws on copyright, trademarks, plagiarism and fair use.
- **Inform our [*PR/Marketing department*]** when you're about to share any major-impact content.
- **Avoid deleting or ignoring comments** for no reason. They should listen and reply to criticism.
- **Never post discriminatory, offensive or libelous** content and commentary.
- **Correct or remove** any misleading or false content as quickly as possible.

Disciplinary Consequences

We'll monitor all social media postings on our corporate account.

We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media at work.
- Disclosing confidential information through personal or corporate accounts.
- Directing offensive comments towards other members of the online community.

If you violate this policy inadvertently, you may receive a reprimand. We expect you to comply after that, or stricter disciplinary actions will apply.

Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.