INSIDER PRO
FROM IDG

EXPERT INSIGHT INTO HOW TECHNOLOGY DRIVES BUSINESS

INSIDER EXCLUSIVE

HOW TO CREATE AN EFFECTIVE SECURITY POLICY

Plus, templates for security policy on passwords, acceptable use, email, access control, BYOD and incident response.

BY NEAL WEINBERG

IDGInsiderPro.com

POWERED BY CIO COMPUTERWORLD CSO InfoWorld NETWORKWORLD

HOW TO CREATE AN EFFECTIVE SECURITY POLICY

BY NEAL WEINBERG

ANYONE CAN GO ONLINE AND DOWNLOAD A SET OF GENERIC, COOKIE-CUTTER SECURITY POLICIES. And while the adoption of those templates might enable an auditor or a compliance officer to check the box that says the organization has a security policy in place, it doesn't do anything to make the company any less vulnerable to attack.

In order to implement a truly effective security policy, organizations should take a comprehensive approach that includes building support from upper management, making sure end users are on board and understand the importance of complying with security policies, providing continuous education, and enforcing policies in a serious way.

In other words, companies need to build an enterprise-wide security culture, which is easier said than done.

To comment on this story, visit Insider Pro's Twitter page.

The first problem is that unless security policies are constantly reinforced through education, testing and periodic re-certification, many employees simply forget the rules. An even bigger problem is employees deliberately skirting strict security guidelines because the policies might be perceived as unnecessarily slowing them down or getting in the way of them doing their job. So, an end user might share their password with a contractor, for example, out of expediency.

Shadow IT is another situation in which employees sidestep the normal IT procurement and security procedures and avail themselves of cloud-based productivity, storage and collaboration applications that IT isn't even aware of.

In this environment, organizations need to take a thoughtful, measured approach to writing and implementing security policies that strike a balance between protecting the organization and not being so onerous that employees reject or ignore the policies.

How to develop a security policy

Developing a security policy starts with identifying a set of clear goals and objectives, defining the scope of the policy in terms of who should be covered, and pinpointing what data needs to be secured.

In order to build consensus, it's important to be inclusive, to enable everyone who will be impacted by the policies to have a voice in defining them.

Companies also need to understand the current state of their security defenses. For example, a vulnerability assessment or penetration testing exercise will establish where the holes are. An understanding of regulatory obligations is also important.

And organizations need to conduct an honest evaluation of their existing culture; are existing rules strictly enforced or are things typically pretty lax. In other words, how likely is it that the organization will face significant pushback from employees if it tries to impose new prohibitions against practices that were previously allowed, like accessing social media sites during work hours.

Companies also need to make sure that security policies are written in clear, understandable language, not convoluted legalese. And the way that companies execute their security education programs needs to reflect the different ways that people learn. For example, instead of requiring that employees physically attend a classroom session conducted by an HR person or security professional, companies could provide online, self-directed learning experiences.

Once a company makes the decision to write a set of security policies, the next step is to prioritize, because there are literally scores of policy templates that cover everything from a "clean desk" policy to rules on how to retire old equipment to policies covering various types of disasters, including pandemics. Companies will want to identify the most critical pain points and avoid overwhelming employees with too many policies.

For most companies, the top six policies would cover password generation and protection, acceptable use of corporate resources, email and other electronic communications, access control, BYOD and incident response.

And keep in mind, these templates are just a framework. Each company needs to customize these templates to suit their unique requirements.

Neal Weinberg *is an award-winning technology journalist and a regular contributor to Insider Pro. You can contact him at neal@misterwrite.net*

AF-STUDIO / GETTY IMAGES

TEMPLATE FOR

PASSWORD/PASSPHRASE PROTECTION POLICIES

THERE IS A BIT OF A CONTROVERSY GOING ON TODAY WHEN IT COMES TO PASSWORDS. Most companies require that users change their passwords on a regular basis, typically every 90 days. But new guidance from NIST recommends that companies not require a change unless a password has been compromised. And Microsoft recently announced that it was removing the forced expiration of passwords in Windows 10. The argument in favor of eliminating mandatory password changes is that forcing people to change passwords frequently encourages them to re-use the same passwords or patterns across multiple websites. Plus, most passwords are stolen through phishing attacks, and a forced password change won't prevent that. However, many security managers are comfortable with the practice and are reluctant to drop it. In any event, here's a template for password security policies that incorporates the latest thinking on passwords/passphrases.

1. **The more characters, the stronger the password,** so passwords should be at least 14 characters. Passphrases consisting of multiple words are recommended.
2. **Every work account should have a different,** unique password.
3. **Users may not use work** related passwords for personal accounts.
4. **Employees should use password manager software** provided by the organization.
5. **Whenever possible,** multi-factor authentication should be used.
6. **Passwords should be changed only** when there is reason to believe a password has been compromised.
7. **Passwords must not be shared** with anyone, including coworkers and supervisors.
8. **Passwords should not be inserted** into email messages.
9. **Do not use the "remember password" feature** of web browsers or other applications.
10. **Any user suspecting that their password may have been compromised** must report the incident and change all passwords.
11. **The Infosec team will verify compliance,** and employees found to have violated the policy may be subject to disciplinary action.

LORD_ZIGNER / GETTY IMAGES

TEMPLATE FOR

ACCEPTABLE USE POLICIES

THE FIRST CONTACT THAT NEW EMPLOYEES HAVE WITH SECURITY POLICY IS WHEN THEY ARE REQUIRED TO SIGN AN ACCEPTABLE USE AGREEMENT AS THEY TAKE POSSESSION OF COMPANY-OWNED ELECTRONIC DEVICES. Since there is some expectation on the part of employees that they will be able to access corporate resources while at home or on the road, it is important that enterprises think long and hard about acceptable use policies and how those policies will balance security concerns with the ability of employees to do work at odd hours from locations outside of the corporate office. Here is a sample template:

1. **Generally speaking, computer equipment, software, storage media, and corporate email accounts** are the property of the company and should be used for business purposes only.
2. **Employees have a responsibility to protect proprietary** information stored on corporate devices.
3. **Employees should promptly report the theft**, loss or unauthorized disclosure of proprietary information.
4. **Individual departments are responsible** for creating guidelines on the personal use of corporate resources.
5. **All mobile devices that connect** to the corporate network must comply with access policies.
6. **Postings on social media** should contain the disclaimer that opinions expressed are strictly those of the writer.
7. **The following activities are prohibited:** violation of copyright, patent or other intellectual property, using pirated software, introduction of malicious programs into the network, revealing your password to others, including family members, sending emails that could be construed as spam or harassment.
8. **Companies may also want to create** application whitelists and blacklists which specify which applications employees can access and which ones are prohibited.

LORD_ZIGNER / GETTY IMAGES

TEMPLATE FOR

EMAIL SECURITY POLICIES

AN ESTIMATED 90% OF SECURITY BREACHES START WITH A SUCCESSFUL PHISHING ATTACK, SO HAVING A STRONG EMAIL POLICY REINFORCED WITH CONTINUOUS EDUCATION IS A KEY PIECE OF ANY SECURITY POLICY INITIATIVE. An estimated 90% of security breaches start with a successful phishing attack, so having a strong email policy reinforced with continuous education is a key piece of any security policy initiative. Many companies augment their efforts to protect email with a program of sending out fake phishes in order to keep employees on their toes and to help them identify what a phishing attempt looks like.

1. **Emails are for business use.** That seems obvious, but it needs to be spelled out. Companies also need to make a decision on whether any and all personal use of business email accounts is strictly prohibited or whether there is some flexibility in the policy that allows employees to use business email under certain conditions and limitations.
2. **Employees are not allowed to use business email to sign up** for accounts unrelated to work.
3. **Emails are company property** and can be legally monitored and viewed by the employer.
4. **Do not open** email attachments from unknown sources.
5. **Never click on links** that appear in emails.
6. **Encrypt any proprietary** or sensitive information sent via email.
7. **Email messages may not be used to harass**, make threats, be offensive or disruptive.
8. **Email messages may not include language or images** related to race, gender, sexual orientation, pornography, religious or political beliefs, national origin or disability.
9. **Employees should report the receipt of inappropriate** or suspicious emails with a supervisor or manager.
10. **Email policy should define** what emails should be retained and for how long.

LORD_ZIGNER / GETTY IMAGES

TEMPLATE FOR

ACCESS CONTROL POLICIES

ACCESS CONTROL IS ANOTHER AREA WHERE THERE IS AN INTERESTED DEBATE GOING ON OVER WHICH APPROACH IS BEST – the popular and widely-deployed role-based access control or attribute-based access control, which is even more granular in terms of what specific resources an employee can access. Whether you're using role-based or attribute-based methods, here's a general template for authentication and authorization.

1. **Secure remote access must be strictly controlled with encryption (VPN)**, strong passphrases and multi-factor authentication.
2. **Authorized users shall protect their login and password**, even from family members.
3. **Remote users shall ensure that their device is not** connected to any other network.
4. **All hosts that are connected to the corporate network** via remote access technologies must use the most up-to-date anti-virus software.
5. **Remote access logs must be kept for a period** of at least 90 days and reviewed regularly.
6. **Users must exercise caution when connecting from public venues** like airports, coffee shops, etc., and must not connect to the internal network from an unsecured, public network.
7. **Access accounts used by third parties** must only be enabled during the required time period and must be disabled immediately thereafter.
8. **Authorized third-party users must be required to authenticate** before being allowed to access restricted information.

LORD_ZIGNER / GETTY IMAGES

TEMPLATE FOR

INCIDENT RESPONSE (IR) POLICY

INCIDENT RESPONSE IS THE ONE POLICY THAT COMPANIES HOPE THEY NEVER HAVE TO USE, but it is critically important to have an effective IR policy teed up and ready to go in the event of a security breach. An effective response to an incident can help companies stop the bleeding, identify the root cause of the incident and shore up the company's defenses to help block future attacks.

1. **Be prepared by identifying** policies, tools, procedures, effective governance and communication plans. Post-mortem analyses from prior incidents should form the basis for continuous improvement. A multi-disciplinary IR team including employees involved in communications, business continuity, legal and insurance should be created and should conduct mock incident response drills.
2. **Detection of an event can occur through internal security tools,** but more often than not companies are notified by an outside party. A rapid response team needs to conduct initial classification of the incident.
3. **Containment is the triage phase where the affected host or system is identified**, isolated or otherwise mitigated, when affected parties are notified and when the investigative status is established. This phase includes evidence handling and communication of the event to the appropriate parties.
4. **Investigation is the phase where security personnel determine** the priority, scope, and root cause of the incident.
5. **Remediation is the post-incident repair of affected systems,** analysis that confirms the threat has been contained and the determination of whether there are regulatory requirements to report the incident.
6. **Recovery is the analysis of the incident** for its procedural and policy implications, the gathering of metrics, and the incorporation of lessons learned into future response activities and training.
7. **Companies also need to have contingency plans in place** in the event that an insider who is part of the incident response team is suspected of being responsible for the event, either intentionally or by mistake.

LORD_ZIGNER / GETTY IMAGES

TEMPLATE FOR

BYOD SECURITY POLICIES

BYOD HAS BECOME AN ACCEPTED FACT OF LIFE AT MOST COMPANIES, as employees make the case that allowing them to do work on their smartphones or other mobile devices improves productivity. In fact, simply being mobile can increase productivity by up to 34%, according to a recent Frost & Sullivan survey. In another study, well-implemented BYOD policies have accounted for average company savings of up to $350 per employee per year. But BYOD also opens up new attack vectors and vulnerabilities that must be addressed. Putting together a BYOD security policy requires careful consideration of a variety of core issues that can only be decided by a team that includes business managers, IT execs, HR, and the legal team.

1. **Companies should specify and limit what devices can connect to the network** and also stipulate that only current versions of operating systems, such as Android or iOS, are allowed.
2. **Companies should also require that employee-owned devices have** mobile device management software installed before they can access the network.
3. **Devices must store all user-saved passwords in** an encrypted password store.
4. **Devices must be configured with a secure password that complies** with the company's password policy. This password must not be the same as any other credentials used within the organization.
5. **Users must only load data essential to their job** onto their mobile device.
6. **Users must report all lost or stolen devices** to IT immediately.
7. **If a user suspects unauthorized access** to company data via a mobile device, they must report the incident.
8. **Devices must not be jailbroken, rooted or have any software/firmware installed** that is designed to gain access to prohibited applications.
9. **Users must not load** pirated software or illegal content onto their devices.
10. **Applications must only be** installed from approved sources.
11. **Devices must be kept up to date** with manufacturer or network provided patches.
12. **The company will/will not reimburse** the employee for a percentage of the cost of the device or the cost of the service plan.
13. **The employee's device may be remotely wiped if the device is lost**, the employee terminates employment, or IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
14. **The employee is expected to use the device in an ethical manner** at all times and adhere to the company's acceptable use policy.
15. **The employee assumes full liability** for the loss of company and/or personal data due to an OS crash, errors, bugs, viruses and any other hardware or software failures that render the device unusable.

LORD_ZIGNER / GETTY IMAGES