Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-sec-policy

IT SECURITY

Security policy: who decides, who acts and who is accountable

The Department of Everything was preparing for a security audit. The Manager called a meeting and placed a binder the size of a small refrigerator on the table. Its gold label read: “SECURITY POLICY — FINAL VERSION, VOLUME I OF XII.” Agnes from Accounting moved her mug. Gregory looked for the emergency exit. 📋🔐🤣

— AS OF TODAY, WE ARE SECURE! — the Manager announced.

— What has changed? — Agnes asked.

— WE PRINTED THE POLICY!

— The accounting passwords?

— UNCHANGED!

— The backups?

— ALSO UNCHANGED!

— Who reports an incident?

— IT'S IN THE BINDER!

Gregory opened volume one. The first page said: “Everyone is responsible for security within their area of competence.”

— Wonderful. When something happens, everyone will wait for somebody else.

A binder won't stop a burglar

The Manager lined up the documents like fortifications.

— POLICY! PROCEDURE! INSTRUCTIONS! RULES FOR USING THE RULES!

— What about instructions for opening the binder? — Agnes asked.

— VOLUME SEVEN!

Gregory wrote three questions on the board: “What?”, “Who?” and “How?”.

An information security policy defines objectives, principles and accountability. Procedures describe actions; instructions can explain particular tasks. The documents should fit the real organisation, not somebody's imaginary perfect company.

— Does signing a fire safety notice put out a fire? — Gregory asked.

— NO, BUT WE HAVE A SIGNATURE!

— A signature proves approval, not effectiveness. We'll discover that when we see what people actually do.

Everybody is responsible, so nobody is

The records room lock broke. The Manager emailed everyone: “Fix urgently!” Everyone read it. Nobody moved.

— BUT I GAVE AN ORDER!

— To everybody — Agnes replied. — Who was supposed to do the work?

Gregory outlined four roles.

— We need to know who makes a decision, who performs the task, whom to consult and whom to inform. You might use a RACI chart or a simpler table. What matters is clear responsibility.

— I'LL APPROVE EVERYTHING!

— Then every password reset waits for you even when you're on holiday? Management sets priorities and funds work, system owners define requirements, administrators implement controls, and staff follow rules and report problems.

— WHAT ABOUT AGNES?

— She knows what happens if payroll is down. You can't assess business risk without involving the people who own the work.

— EVERYTHING IS CRITICAL! — the Manager shouted.

— Then nothing takes priority — Agnes replied.

Top-secret tomato soup

The policy classified every document as confidential, including the cafeteria menu.

— Do we need written approval to learn what's for lunch? — Agnes asked.

— SECURITY REQUIRES SACRIFICE!

— Protection should be proportionate — Gregory said. — A public price list, an internal schedule, customer information and confidential financial records require different safeguards. Information classification helps determine access, storage and sharing rules.

— SO CAN WE MAKE THE MENU PUBLIC?

— Unless it's a military operation plan — Agnes replied.

— WHO CLASSIFIED THE SOUP?!

— You did. Yesterday at 2:07. I have your signature.

You can't ban risk by decree

The Manager ordered protection against every possible threat: criminals, floods, power failures, mistakes and meteorites.

— BAN METEORITES!

— They haven't signed the policy — Agnes pointed out.

Gregory opened the risk register.

— We identify what matters, what might happen, its probability and consequences, and what level of risk the organisation is prepared to tolerate. Then we select controls. Risk may be reduced, avoided, sometimes transferred or consciously accepted.

— WHO APPROVES ACCEPTANCE?

— An authorised risk owner. Administrators can explain technical exposure and options, but shouldn't be left alone to decide what losses the business can tolerate.

— WHAT IF I WRITE “IT'LL PROBABLY BE FINE”?

— That's not somebody's name.

Administrator privileges for everyone!

At ten, the Manager announced his access reform.

— TO AVOID BLOCKING ANYBODY, EVERYBODY GETS ADMIN RIGHTS!

— Or we could confiscate all computers to prevent mistakes — Agnes suggested.

— AN EXCELLENT IDEA!

— Both are bad — Gregory interrupted. — The principle of least privilege gives people the access their jobs require, no more. Accountants don't need to administer every server, and administrators don't automatically need to read private mail.

Access should be approved, reviewed and revoked when duties change or staff leave. Emergency access needs planning too, or people will invent secret shortcuts.

— I ALREADY HAVE ONE! MASTER KEY UNDER A FLOWERPOT!

— We tried that at the **Golden Password Hotel** — Gregory sighed. — It's still a terrible idea.

The exception that lasts forever

At noon, the network printer stopped responding. The Manager demanded that all protection be disabled immediately.

— DISABLE THE FIREWALL! I NEED MY REPORT!

— First we'll identify which traffic is required and what changed, then make a carefully scoped exception if needed — Gregory replied.

— WHY ALL THE TROUBLE?

— Change policy should identify who requests, assesses risk, approves, implements, tests and rolls back a change. Exceptions need a scope, owner and often an expiry date.

Agnes held up the previous change request.

— This says “Open everything because it doesn't work.” No date or rollback plan.

— WHO SIGNED THAT?!

— You did. In the Republic of Packets.

— Just like our **firewall adventure** — Gregory smiled.

Incidents don't arrive with an INCIDENT label

At 12:43, Agnes got an urgent request to send payment to a supplier's new account. Instead of transferring money, she reported it.

— WHAT IF IT WAS REAL? — asked the Manager.

— Then we'll check. Employees don't have to conduct a full investigation. They need to know how to report suspicious events quickly — Gregory explained.

An incident procedure defines reporting channels, responsible people, priorities, evidence preservation and contact arrangements. It should be tested before a crisis.

— I'LL MAKE A “NOT AN INCIDENT” STAMP!

— A stamp is not an assessment. This message looks like the examples in our **phishing article**.

Backups, according to volume nine

The auditor asked when data had last been successfully restored from backup.

— VOLUME NINE SAYS WE MAKE BACKUPS!

— When did we test restoring them? — Agnes asked.

The silence lasted until the screensaver appeared.

— A procedure for making copies is not proof that recovery works — Gregory said. — We need schedules, tests, responsible staff and protected backup storage. Training is similar: a read receipt doesn't prove somebody knows how to recognise a threat.

— BUT WE SENT EVERYONE THE POLICY!

— Do they know what to do after losing a laptop or receiving a scam message? We have separate stories about **backups** and **security fundamentals**. Policy should produce action, not just a PDF attachment.

Auditors want evidence, not paper weight

The Manager proudly arranged twelve binders by height.

— OUR SECURITY SYSTEM WEIGHS SEVENTEEN KILOGRAMS!

— May I see the latest access review? — the auditor asked.

— VOLUME THREE!

— The backup restoration test result?

— VOLUME NINE!

— Did anyone actually perform the work?

Silence. Agnes arrived with change records, a list of responsible people and a restoration test report created after that morning's discussion.

— That's the point — the auditor said. — Documents state intentions. Records and practice demonstrate execution. Passing an audit doesn't guarantee that nothing bad will happen either.

— WHAT ABOUT MY BINDERS?!

— Keep them, but make sure people can find an answer in less than three days.

A policy people can actually use

That evening, Agnes prepared a shorter guide with clear links to procedures. It named owners, reporting routes, exceptions and review dates.

— So nobody has to memorise twelve volumes? — the receptionist asked.

— They need to know how to work safely, what not to do and where to find help — Gregory said. — Policies should be understandable, accessible, current and suited to the organisation.

— What if our systems change? — Agnes asked.

— Review the policy after significant changes and on a planned schedule. It shouldn't describe a server retired five years ago.

— ONE RULE: “PLEASE THINK”! — the Manager proposed.

— Helpful advice, but not a substitute for permissions, responsibilities and procedures.

— THEN I'LL STAMP IT!

He slammed his stamp onto the desk. A note fell from the binder: “Administrator password — ask the Manager.”

— SEE?! CENTRAL ACCOUNTABILITY!

— No — Agnes said. — Another corrective action.

Security policy is not a shield made of paper. It must set practical rules, assign decision owners and help people act. Too complicated becomes dead weight, too vague answers nothing, and ignored rules offer only an illusion of protection.

Minutes of the Department of Everything: the policy has an owner, exceptions have expiry dates, incidents have a reporting contact and backups have a restoration schedule. Twelve binders remain in the archive. The Manager has requested a thirteenth: “Policy Against Excessive Policies.” It is awaiting his signature. 📋🤣❤️