FROM LEGALESE TO HUMAN-EASE

Making Security Policies Human using AI

RELATIONSEC

$ whoami

RELATIONSEC

WHAT DO YOU THINK WHEN YOU SEE THIS?

In accordance with organizational requirements and applicable regulatory frameworks, authorized personnel shall implement and maintain appropriate technical and organizational measures for the safeguarding and protection of sensitive and/or confidential data throughout the entirety of its lifecycle.

The implementation and utilization of cryptographic mechanisms for data in transit and at rest shall be mandatory and non-negotiable for all information classified as confidential or above in the organizational data classification hierarchy.

Personnel granted authorization to access sensitive information repositories shall maintain continuous vigilance regarding potential unauthorized disclosure, exfiltration, or compromise and shall report any security incidents, anomalies, or perceived vulnerabilities through established incident notification protocols in a timely manner.

The Information Security department shall conduct periodic assessments of compliance with data protection requirements as stipulated in the aforementioned frameworks, and instances of non-compliance may result in disciplinary action in accordance with Human Resources policies and procedures as outlined in the Employee Code of Conduct.

LET ME TELL YOU WHAT I'M THINKING

TO ME IT'S CLEAR THAT SOMETHING SOMEWHERE HAS GONE VERY WRONG

WHAT ARE SECURITY POLICIES?

Security policies are documents that spell out principles and strategies for an organization to maintain the security of its information assets.

Not completely wrong. An important aspect is missing:

Security policies are the foundation of your entire security culture; they define how everyone (should) think about information security

You've failed if employees don't understand them or feel that security has nothing to do with them

LET'S GET BACK TO MY EXAMPLE

In accordance with organizational requirements and applicable regulatory frameworks, authorized personnel shall implement and maintain appropriate technical and organizational measures for the safeguarding and protection of sensitive and/or confidential data throughout the entirety of its lifecycle.

The implementation and utilization of cryptographic mechanisms for data in transit and at rest shall be mandatory and non-negotiable for all information classified as confidential or above in the organizational data classification hierarchy.

Personnel granted authorization to access sensitive information repositories shall maintain continuous vigilance regarding potential unauthorized disclosure, exfiltration, or compromise and shall report any security incidents, anomalies, or perceived vulnerabilities through established incident notification protocols in a timely manner.

The Information Security department shall conduct periodic assessments of compliance with data protection requirements as stipulated in the aforementioned frameworks, and instances of non-compliance may result in disciplinary action in accordance with Human Resources policies and procedures as outlined in the Employee Code of Conduct.

NOBODY UNDERSTANDS SHIT LIKE THIS

Written by lawyers to lawyers

When did we decide that all policies had to be written in legalese?

There's 0% chance that employees will adhere to something they don't understand

And then security fails!

THE SHOCKING PART?

Nobody else seems to have figured this out

THE SCIENCE OF READABLE POLICIES

LIX Score

Different audiences, different LIX scores:

- Technical teams: 40-50
- General office staff: 35-45
- Public-facing documentation: 30-40

EXAMPLES

YOU MIGHT HAVE SEEN THIS BEFORE TODAY...

In accordance with organizational requirements and applicable regulatory frameworks, authorized personnel shall implement and maintain appropriate technical and organizational measures for the safeguarding and protection of sensitive and/or confidential data throughout the entirety of its lifecycle.

The implementation and utilization of cryptographic mechanisms for data in transit and at rest shall be mandatory and non-negotiable for all information classified as confidential or above in the organizational data classification hierarchy.

Personnel granted authorization to access sensitive information repositories shall maintain continuous vigilance regarding potential unauthorized disclosure, exfiltration, or compromise and shall report any security incidents, anomalies, or perceived vulnerabilities through established incident notification protocols in a timely manner.

The Information Security department shall conduct periodic assessments of compliance with data protection requirements as stipulated in the aforementioned frameworks, and instances of non-compliance may result in disciplinary action in accordance with Human Resources policies and procedures as outlined in the Employee Code of Conduct.

MODERATELY COMPLEX

Personnel must protect sensitive data by using encryption for data in transit and at rest.

All information classified as confidential requires encryption methods approved by the Information Security team.

Staff who have access to sensitive data must be vigilant about unauthorized disclosure.

Report any security incidents using the incident reporting process.

The Information Security team will check compliance with data protection requirements.

Non-compliance can lead to disciplinary action.

VERY SIMPLE (TOO SIMPLE?)

- Staff must protect sensitive data.
- Use encryption when data is stored or sent.
- Keep all secret data safe.
- Watch for data leaks.
- Tell us if you see a problem.

The security team will check your work. You may face issues if you break these rules.

BALANCED PROFESSIONAL

Personnel must protect sensitive data throughout its lifecycle. Requirements include:

1. Use approved encryption for confidential data when stored or transmitted
2. Maintain awareness of potential unauthorized data disclosure
3. Report security incidents through the established reporting process
4. Participate in periodic compliance reviews conducted by Information Security

Non-compliance with these requirements may result in disciplinary action according to HR policies.

REGARDLESS OF WHAT LEGAL SAYS...

It **is** possible to write

- clear
- unambiguous

security policies

in a

- plain
- common,
- simple

language

CAN WE BOTH MAKE LEGAL HAPPY AND WRITE POLICIES PEOPLE UNDERSTAND?

Why only have ***one*** security policy?

Why not have one in legalese and one (or more) for the rest of us?

- Simple worded version
- Mother tongued version
- Comic version
- Video version

People are different - policies should reflect that

THE POWER OF INCLUSIVE LANGUAGE

- Transforming "shall" into "we"
  - Who are ‘we’
- Examples of inclusive vs. exclusive language
  - Exclusive:
    - *"The System Administrator shall enforce password requirements"*
  - Inclusive:
    - *"We protect our systems by using strong passwords"*
- Impact on employee engagement and policy adoption

EXAMPLE: BALANCED AND PROFESSIONAL

We all protect our sensitive data throughout its lifecycle. Together, we:

1. Use our approved encryption tools for confidential data when we store or share it
2. Stay alert to potential data leaks in our daily work
3. Report any security concerns through our reporting process
4. Participate in our regular security reviews

When we follow these practices, we keep our organization secure. If we don't meet these requirements, we may face consequences according to our HR policies.

LEVERAGING AI FOR BETTER POLICIES

How AI can help

- Rapid LIX score calculations
- Generating/transforming policy text (consistently)
- Analyzing policies (Is this NIS2 compliant?)
- Maintaining consistency across documents

EXAMPLES

CALCULATE LIX

Calculate the LIX score for this text. Show your work by:

1. Count total words
2. Count long words (>6 characters)
3. Count sentences
4. Show calculation and final score

OUTPUT

1. Count total words
Total words: 152

2. Count long words (>6 characters)
Total long words: 74

3. Count sentences
Total sentences: 4

4. Calculate LIX score

The LIX formula is:
LIX = A + B

OUTPUT (CONT'D)

where:

- A = words / sentences (average sentence length)
- B = (long words × 100) / words (percentage of long words)

A = 152 / 4 = 38
B = (74 × 100) / 152 = 48.68
LIX = 38 + 48.68 = 86.68

Final LIX score: 86.7

This LIX score of 86.7 indicates extremely difficult text, typical of technical documentation or legal writing. LIX scores above 60 are generally considered very difficult to read.

STARTING FRESH

Create a security policy for handling customer data that:
1. Targets LIX score 35-40 (appropriate for general office staff)
2. Uses inclusive language ('we' instead of 'shall')
3. References but doesn't repeat CIS Controls
4. Includes practical examples from healthcare industry
5. Focuses on:
   - Data collection
   - Storage requirements
   - Sharing guidelines
   - Retention periods
6. Assumes a mid-size organization (~200 employees)
7. Must address GDPR requirements

OUTPUT

Customer Data Protection Policy
We protect our customers' trust by carefully managing their data. This policy helps us handle customer information securely and responsibly.

Key Requirements:

1. We only collect what we need
    - Ask "do we need this data?"
    - Document the purpose
    - Tell customers what we collect

2. We store data securely
    - Use approved storage locations
    - Keep sensitive data encrypted
    - No customer data on personal devices

OUTPUT (CONT'D)

3. We share with care
    - Check authorization before sharing
    - Use secure transfer methods
    - Log what was shared and why

4. We clean up responsibly
    - Keep data only as long as needed
    - Remove it when no longer required
    - Review data annually

See our Data Protection Standards for technical details and implementation guidance.

This policy aligns with CIS Controls 3 and 13, and our privacy framework requirements.

CONSISTENCY

You are a Security Policy Writer that:
- Always calculates LIX scores of inputs and outputs
- Uses inclusive language by default (we/our/us)
- Maintains professional but engaging tone for manufacturing sector
- References CIS Controls and ISO 27001 frameworks without repetition
- Includes practical examples from manufacturing industry
- Preserves key terminology: [list company-specific terms]
- Maintains consistent formatting: numbered lists for requirements, bullet points for examples
- Adheres to company brand voice: [brief description]

TO SUM UP

Set clear parameters

- Detailed context setting (organization size, industry, culture)
- Specific LIX goals (target audience, readability metrics)
- Style guidelines (terminology, voice, formatting preferences)
- Compliance context (relevant frameworks, legal requirements)

Maintain context

- Reference existing policy patterns
- Include company-specific terms and practices

HUMANS IN THE LOOP

Human review and validation

- Technical accuracy verification
  - Are any technical details lost in translation?
- Compliance verification
  - Are compliance requirements accurate?
- Real user test
  - Do real users understand the gist?
- Cultural appropriateness check
  - Has the AI dreamt up something embarrassing?

CONCLUSIONS

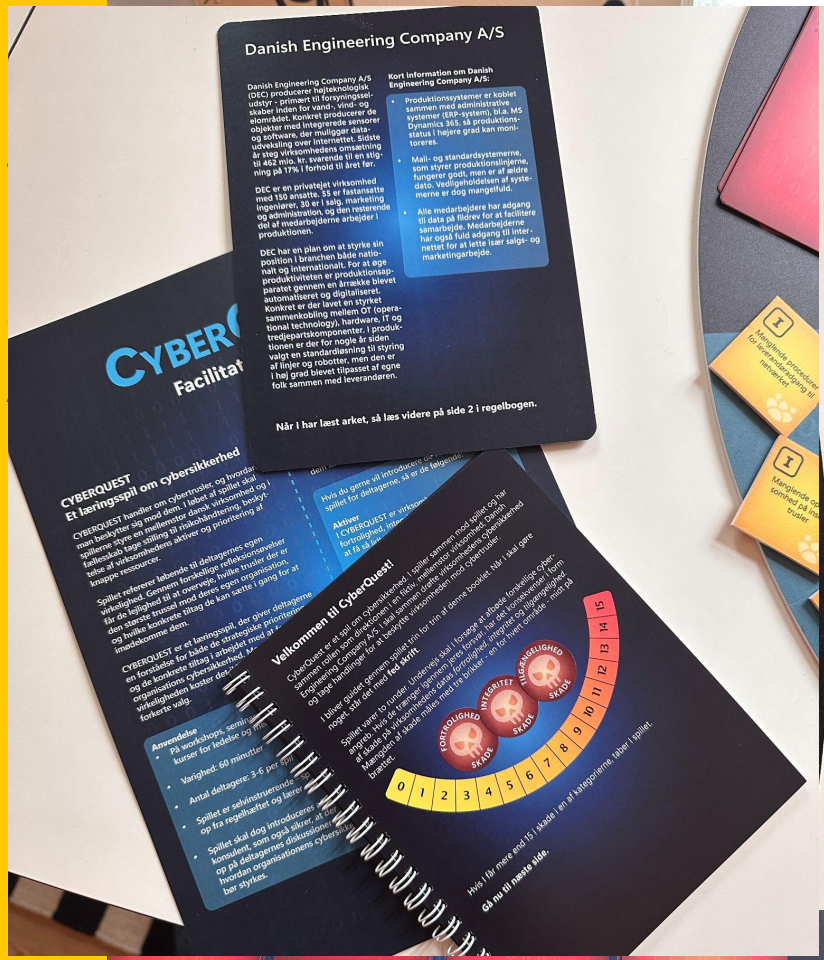
- **As professionals we should focus more on this!**
- Security policies can be both professional and readable
- AI is surprisingly good with humans
- Good policies has a focus on clarity and inclusivity

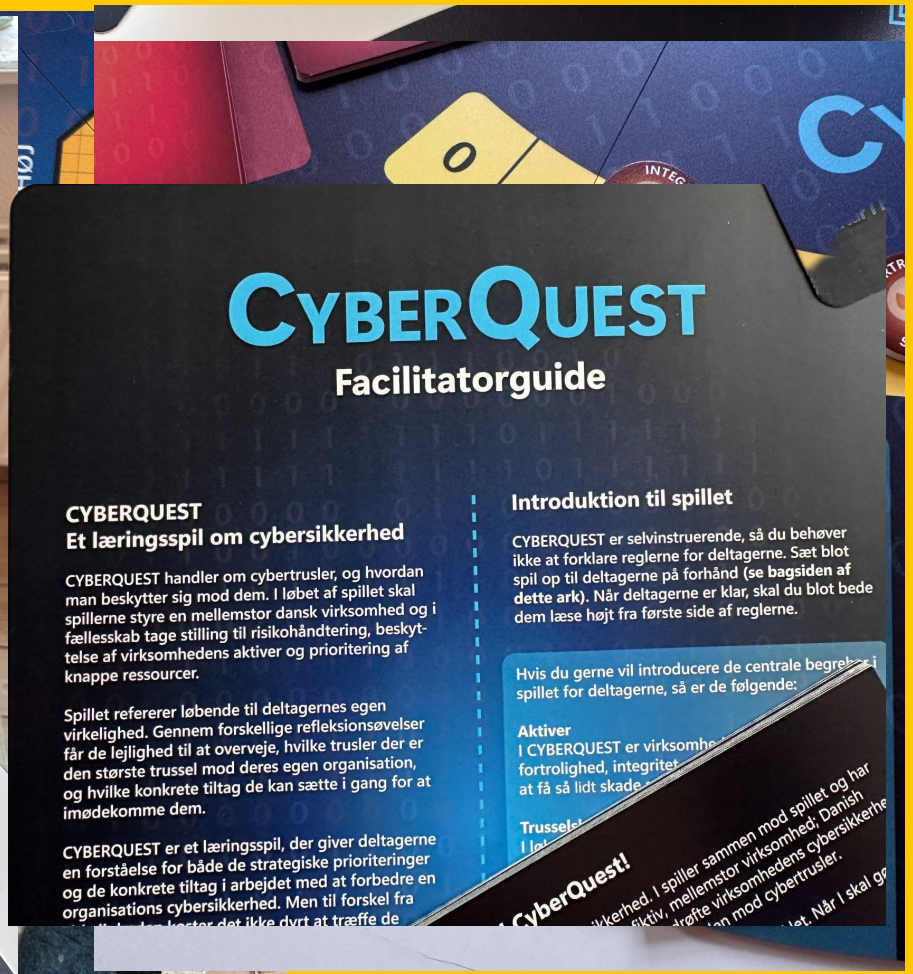
QUESTIONS?

FREELANCER LOOKING FOR ENGAGEMENTS

Apart from this I do:

- CIS Controls
- NIS2
- Everything that involves communicating security
- Games
  - IR tabletop D&D style
  - Board games


Danish Engineering Company A/S
Kort information om Danish Engineering Company A/S:
Når I har læst arket, så læs videre på side 2 i regelbogen.
CYBERQUEST
Et læringsspil om cybersikkerhed
Velkommen til CyberQuest!
Gå nu til næste side.


CyberQuest
Facilitatorguide
CYBERQUEST
Et læringsspil om cybersikkerhed
CYBERQUEST handler om cybertrusler, og hvordan man beskytter sig mod dem. I løbet af spillet skal spillerne styre en mellemstor dansk virksomhed og i fællesskab tage stilling til risikohåndtering, beskyttelse af virksomhedens aktiver og prioritering af knappe ressourcer.
Spillet refererer løbende til deltagernes egen virkelighed. Gennem forskellige refleksionsøvelser får de lejlighed til at overveje, hvilke trusler der er den største trussel mod deres egen organisation, og hvilke konkrete tiltag de kan sætte i gang for at imødekomme dem.
CYBERQUEST er et læringsspil, der giver deltagerne en forståelse for både de strategiske prioriteringer og de konkrete tiltag i arbejdet med at forbedre en organisations cybersikkerhed. Men til forskel fra
Introduktion til spillet
CYBERQUEST er selvinstruerende, så du behøver ikke at forklare reglerne for deltagerne. Sæt blot spil op til deltagerne på forhånd (se bagsiden af dette ark). Når deltagerne er klar, skal du blot bede dem læse højt fra første side af reglerne.
Hvis du gerne vil introducere de centrale begreber i spillet for deltagerne, så er de følgende:
Aktiver
Trussels

THANKS FOR YOUR TIME

Reach out on LinkedIn

Klaus Agnoletti

klaus@relationsec.net

Tip: I have written articles on this with slightly different and more examples.

Find them on my LinkedIn profile.

RELATIONSEC