

# The top six reasons security policies don't work

**A Secoda white paper**  
**April 2003**

When something goes wrong, or an important defence isn't in place, the organisation's security team try to find out the reasons. Why haven't staff implemented those carefully-crafted policies?

The top 6 excuses that information security people hear are:

1. **"What policies? I didn't know where to find them"**
2. **"I didn't know how they affected me"**
3. **"I didn't know *when* I was supposed to use them"**
4. **"I didn't know which policies were most important in tackling risk"**
5. **"I wasn't convinced they were best practice"**
6. **"I didn't have enough guidance and support"**

Any one of these excuses could be enough for that critical employee to disengage from the security process. Together, the six excuses could derail even the best security strategy.

These aren't technological problems. They are problems of communication, awareness and understanding. Let's take a closer look at each of them, and map out a solution.

## 1: "What policies? I didn't know where to find them"

Let's assume the organisation has already written good security policies. There should be no-one who hasn't been told about them, and where to find them.

Where should the policies be?

### **Good**

Online, on intranet sites.  
 Accessible from all parts of the organisation.

### **Bad**

Printed manuals.  
 In the library at Head Office.  
 In the manager's desk drawer.

## **Four steps to kick-start awareness of policies**

1. Highlight them in the induction or orientation process
2. Ensure they are easily locatable in the intranet's navigation or search system
3. Use email with embedded hyperlinks to publicise the location of the most up-to-date policies
4. Repeat the process annually.

## **2. “I didn’t know how they affected me”**

Imagine you had to sift through a hundred, two hundred or more items, to find the issues that were your responsibility. Chances are, only the most dedicated staff will try this. Things get worse when you consider that security policies aren’t the only policies that organisations have. There are also policies relating to health and safety, human resources, and in financial companies, regulatory issues such as money laundering.

People will respond much better if they can say “this is my job, what do I need to know”, and get a personalised report containing just the policies that apply to them. Avoid information overload and compliance will improve.

## **3. “I didn’t know *when* I was supposed to use them”**

In any business process or IT project lifecycle, different things should happen at different times. The security issues when designing a system are different from those when operating a system, for example. So make it easy for staff to pick out just those requirements that matter for the phase of the process that they’re working on right now.

## **4. “I didn’t know which policies were most important in tackling risk”**

Security professionals know that protection measures are rarely “one size fits all”. How you secure a system depends on the assessed level of business risk. So why are so many policies written without any acknowledgement of the risk assessment process?

As a highly simplified example, don’t write a policy that says “All data must be encrypted before transmission...”. This is unlikely to be necessary or practical in all situations. Instead, consider saying something like “All *strictly confidential* data must be encrypted...”. Have a risk assessment process for deciding which data is “strictly confidential” (there are various published methods for this). And make it easy for staff who have already done a risk assessment to use the results to retrieve this particular policy requirement.

## **5. “I wasn’t convinced they were best practice”**

Sometimes things are forced on people “for security reasons” when the actual motivation hasn’t been thought through, or is something else entirely<sup>1</sup>. If people are inconvenienced for what they feel are arbitrary reasons, they won’t lend their support to valid and proportionate security improvements. And when presented with new security policies in the organisation, some people may suspect the security team of just “making them up”.

The security team can avoid the charge of making up arbitrary policies. They can use published sources of best practice, and clearly cross-reference the organisation’s policies with those external sources. The choice of references depends on the organisation. Candidates include: ISO 17799, BS 7799 part 2, NIST publications, COBIT, ISO TR 13335 (GMITS) and the forthcoming GAISP (formerly GASSP).

---

<sup>1</sup> Privacy International’s “Stupid Security” awards provide many examples. See <http://www.privacyinternational.org/activities/stupidsecurity/>

## **6. “I didn’t have enough guidance and support”**

A danger for the security team is that they might publish policies to staff, and then not be able to cope with the demand for further advice and assistance in implementing policy.

No security team has unlimited resources. They must prioritise, and give more attention to the most business-critical problems. But what about everyone else? From the outset, they should be given quality written guidance and detailed standards for implementing policy in a default, best-practice way. There should also be a way for staff to provide feedback on the policies and guidance: what works; what isn’t so clear.

Over time, regular training and awareness-raising will help staff to help themselves, transferring and devolving knowledge, and instilling security as a standard competency within the organisation.

---

Security policy is “core business” for Chief Security Officers, and the foundation for a secure organisation. But these six excuses represent the real problems that CSOs still face when trying to get their message across.

We call the solution “third generation policy awareness”.

### **What is third-generation policy awareness?**

Third-generation policy awareness is the effective way to communicate the organisation’s policies to its staff. People can easily locate the exact policy that relates to a given situation. No more excuses, just total awareness of the relevant policies.

Third-generation policy awareness presents information in a structured and easy-to-use way. It uses web technology to reach all corners of the organisation, and to make it easy for everyone to understand what the organisation expects of them, personally.

The first generation of policy awareness was the printed handbook of policies.

The second generation, most common today, is the classic intranet site. Good for distributing up-to-date information widely – not so good for locating the information you need today, within a tangle of organisational policies and procedures.

The third generation adds database technology, searching based on relevant business context, and interactive compliance tracking to provide complete control over the process. Role-based guidance helps staff achieve real understanding of policies and go beyond mere tick-box compliance.

Third generation policy awareness is not only a solution to an information security problem. The same techniques work for other areas in businesses or in public sector organisations: corporate governance, privacy and data protection, freedom of information, financial services regulations, healthcare and pharmaceutical regulations, health and safety, and many more.

The table overleaf describes the third generation approach, and how it actually makes policies work.

## The evolution of policy awareness

	First generation	Second generation	Third generation
<b>Medium</b>	Printed policies and procedures.	Documents or text published on intranet.	Structured content accessed via intranet portal.
<b>Search facilities</b>	Index and contents within printed documents.	Standard website textual search.	Relevance-based searching, taking account of user role, process phase, risk level and other factors.
<b>Relating to best practices</b>	None, or lists of references.	None, or lists of references or hyperlinks	Two-way online cross-referencing between policies and detail of best practices.
<b>Guidance</b>	None, or general guidance for each policy.	None, or general guidance for each policy.	Detailed guidance for every policy, tailored for each role responsible for implementing the policy.
<b>Feedback</b>	None, or separately via phone, email or internal post.	Via web form, phone, email or internal post.	Via web form that can reference specific policies and collect users' ratings of the policy; also via phone, email or internal post.
<b>Compliance tracking</b>	None, or performed separately.	None, or performed separately.	Integrated. Uses online 'click to accept' features, testing of user awareness, collation of audit results or other mechanisms.
<b>Policy management</b>	Printing and redistribution of revised policies and procedures.	Standard web site authoring and management tools.	Online policy content management tools.
<b>Likely outcome</b>	<b>Poor levels of awareness and compliance. Policies go out of date.</b>	<b>Moderate levels of awareness and compliance. Policies more likely to be up to date.</b>	<b>Good levels of awareness and compliance. Integration of policy considerations into business processes and workflows.</b>

### About Secoda

Secoda is a privately-owned UK company founded by former senior security officers in FTSE 100 and public sector organisations. Secoda's flagship product is **RuleSafe™**, the foremost third-generation policy awareness solution on the market.

RuleSafe enables the people in organisations to achieve real awareness of policies. Its unique personalised reports help people understand exactly what is required of them for each particular task or project they undertake. RuleSafe's expert content and compliance tracking help organisations implement security, privacy, regulatory and governance requirements.