
Developing a Security Policy is a work by Joel Weise and Charles R Martin, both of whom work for Sun Microsystems. In the work which spans 14 pages Martin and Weise explain the steps to developing a thorough security policy.

Throughout the article which contains 5 references Martin and Weise discuss the importance of a security policy for any organisation that use electronic commerce on the internet, for government organisations that want to automate forms processing, as well as any entity that wish to have external exposure of data processing environments. The article also describes the basic steps needed to developing a security policy, including a set of policy components. As well as the article Martin and Weise have also developed a security policy of their own using their steps which can also be found online.

The article itself is very theoretical without getting down to the very specific areas. There are 4 main sections, with each being broken down into subsections. The articles flow is easy to follow and every point is explained without too much trouble. Although none of the sections are in-depth and are really just a summary of how to go about developing a security policy.

Weise and Martin clearly state that “in today's IT environments, data is often one of the most important assets and should be treated accordingly”[1]. That is why they “recommend for security policy development use a data centric model”[1]. This ideal is also one that Sandrine Duflos follows in her PhD. Duflos found that “many problems arise concerning data confidentiality and integrity”[2].

Security Principles are highlighted as well as the goals that Security Principles should be based upon. Weise and Martin describe Security Principles as “an important first step in security policy development”[1] and “are used to define a foundation upon which security policies can be further defined”[1]. They also recommend that to “ensure managements expectations for security and fundamental business requirements are satisfied”[1] that “organisations should evaluate and review these
security principles before and after the development and elaboration of security policies.[1]

In describing Security Policy fundamentals Weise and Martin define that the purpose of a Security Policy is “to inform users, staff, and managers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets” [1]. Rees, Bandyopadhyay and Spafford define Security Policies as “generally high-level, technology neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed, and must not be confused with implementation- specific information”[3].

Weise and Martin also take the stance that a Security Policy is a high level document in describing the goals of a Security Policy, “The goal of the security policy is to translate, clarify and communicate management’s position on security as defined in high-level security principles”[1].

The desirable characteristics that Weise and Martin are after in a Security Policy include the following:

- They must be **implementable** through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
- They must be **enforceable** with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.
- They must clearly define the areas of **responsibility** for the users, administrators, and management.
- They must be **documented**, **distributed**, and **communicated**.

One of the most important issues that Weise and Martin discussed in their document was the fact that the Security Policy needed to take a Holistic Approach. This means that “no one component of a system provides security”. This ideal is also discussed by Duflos. Duflos explains that there is a need for the policy to have three layers: Service Management, Middleware Management and a Network Management layer. With Each layer having a different policy.[2]
Duflos goes on to explain that “at the service management level the goal is to express information in high-level terms understood by end-users”[2]. And that the “purpose of the middleware management level is to provide middleware policy rules including security aspects taking into account the service needs and the end-users requirements. The creation of policies is due to this level”[2]. Whilst at the Network Management Level “the objective is to make the link with the devices”[2].

In Weise and Martins description of the steps that they recommend are needed to develop a Security Policy it reminds one of the structure of the System Development Life Cycle (SDLC) [4]. Weise and Martin have 9 points that they outline must be done when developing a Security Policy [1]. Now by looking closely you can fit each of these different points into a phase in the SDLC. Listed below are the points they make:

1. All responsible organizations and stakeholders are identified and their roles, obligations and tasks detailed
2. The primary business objectives are outlined
3. A list of security principles representing management’s security goals is outlined
4. All applicable data and processing resources are identified and classified
5. A data flow analysis is performed for the primary data classifications, from generation through deletion
6. The primary threats that can reasonably be expected in one’s environment are outlined
7. The primary security services necessary in the environment are identified
8. A generic policy template is constructed
9. A list of security policies is defined

In the Initiation Phase, which is the first phase of the SDLC [4] we create a report on how much the system or in this case a Security Policy, and how viable and what it will cost, as well as other options available. Now this closely relates to the second point that Weise and Martin make.
Whilst Points 1, 3, 4-7 all fit into the second phase of the SDLC which is the Analysis Phase [4]. And finally Points 8 and 9 slot into the Design Phase of the SDLC. Now whilst the last three stages in the SDLC do not fit into the points that Weise and Martin make, The Policy must be Implemented (Implementation Phase), the policy is always reviewed (Review Phase), and the policy always requires maintenance (Maintain Phase) [4].

Now in Rees, Bandyopadhyay and Spafford, they state that their Security Policy was “developed borrowing from both the new product development life cycle, and the systems development life cycle (SDLC)”[3]. Which Rees, Bandyopadhyay and Spafford narrow down into 4 phases [3]:

- Asses Phase
- Plan Phase
- Deliver Phase
- Operate Phase

Weise and Martin obviously know what they are talking about. Their ideas follow what else is out there in the ways of developing a security policy or maybe everyone else follows their ideas. The article is very explanatory without going into too much technical detail.
References


