General Policy Framework Protime

Contents

General

Introduction

At Protime, we want to make it clear to every Protimer which guides and rules everybody must follow, to handle the privacy of our clients, handle the data of our clients, but also internal processes.

For that reason, we have a policy framework. This explains how employees at Protime should work and react. This general policy refers to some more detailed policies or other documents.

Audience

This policy applies to:

- The head office of Protime
- All branches of Protime
- All staff and volunteers of Protime
- All contractors, suppliers and other people working on behalf of Protime

Purpose

This policy gives an overview of the policies used by Protime, mainly to protect customer data in general.

Protime finds security of user and customer data very important. At Protime we look at security as confidentiality, integrity and availability, on a risk based approach. Every year we evaluate the risks in order to take the necessary steps in development, processes or other.
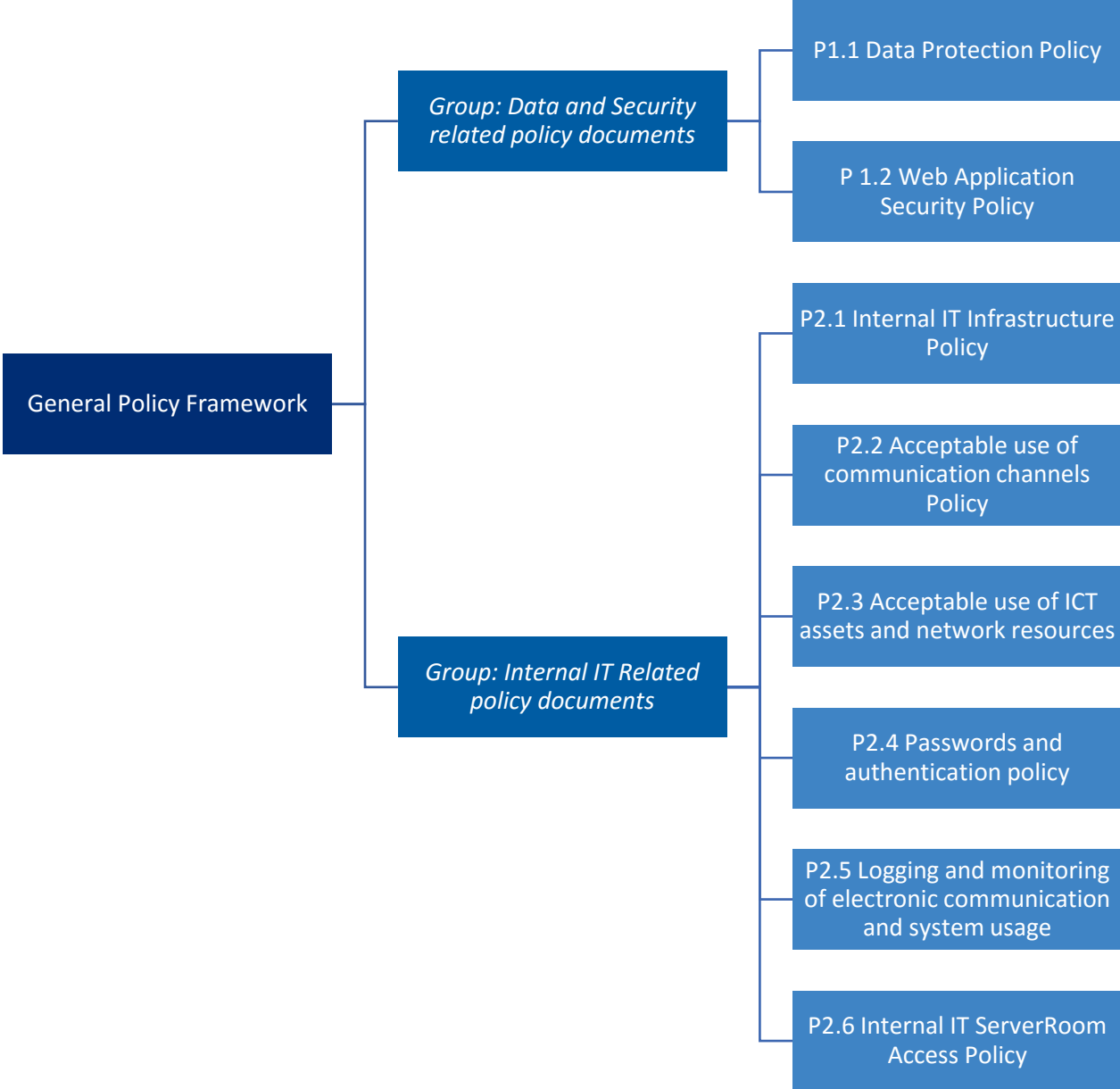
Definition of 'our websites'

See also definition of 'our websites' in the Cookie Statement Protime

Management approval

This policy and al the policies or documents it refers to, are agreed by at executive level. All other information handling documents must be consistent with it.

Overview

This gives an overview how the policy documents are structured:

```
                                        Group: Data and Security      P1.1 Data Protection Policy
                                        related policy documents
                                                                      P 1.2 Web Application
                                                                      Security Policy

                                                                      P2.1 Internal IT Infrastructure
                                                                      Policy

                                                                      P2.2 Acceptable use of
                                                                      communication channels
                                                                      Policy

  General Policy Framework                                            P2.3 Acceptable use of ICT
                                                                      assets and network resources

                                        Group: Internal IT Related    P2.4 Passwords and
                                        policy documents              authentication policy

                                                                      P2.5 Logging and monitoring
                                                                      of electronic communication
                                                                      and system usage

                                                                      P2.6 Internal IT ServerRoom
                                                                      Access Policy
```

Data and Security Related policy documents

P1.1 Data Protection Policy

Protime needs to gather and use certain information about individuals.
These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

P1.2 Web Application Security Policy

Web application vulnerabilities account for the largest portion of attack vectors outside of malware.   It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

This policy describes how Protime protects its websites, searches for a continued improvement of website security, and how it handles issues that are found in the security system.

Internal IT Related policy documents

P2.1 Internal IT Infrastructure Policy

This policy is an internal IT policy which defines anti-virus policy and security issue prevention on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what anti-virus program will be run on the mail server and workstations. It specifies a firewall to protect the internal IT infrastructure. It specifies how windows updates are provided and executed.

P2.2 Acceptable use of internet, email and other communication channels

Internet access, email and other communication channels using Protime networking or computing resources (including but not limited to faxes, telephones, mobile phones, smartphones and multifunctional printing devices), shall be predominantly used for business purposes and must be conducted in a secure, legal and ethical manner. Private use is only allowed if Protime co-workers has consented to logging and monitoring.

P2.3 Acceptable use of ICT assets and network resources

Protime ICT assets and network resources shall be used in a professional way in line with the purpose for which they are intended and in compliance with the Protime security policies. Every Protime co-worker shall practice due care when using company ICT assets.

P2.4 Passwords and authentication policy

Protime co-workers shall use strong passwords and shall adequately protect authentication secrets.

P2.5 Logging and monitoring of electronic communication and system usage

Protime will monitor co-worker behavior to protect the value of Protime information and its ICT assets and improve the quality of its services, while respecting the privacy of Protime co-workers, customers and third parties in accordance with the applicable legislation.

P2.5 Internal IT ServerRoom Access policy

Protime will control and monitor access and conduct to and within the server room.

Roles and responsibilities

Category	Responsible	Accountable	Consulted	Informed
Data Protection of application data	Datacenter team, Support team Development, Consultants	Technology Director	Directors, Teamleads, Product owners	
Data Protection of public website data	Marketing	Marketing Director	Directors	Product owners
Internal IT	Every Protime employee or contractor who uses a Protime computer or server	IT Director	Directors	IT manager
Acceptable use	Every Protime employee or contractor	IT Director	Directors	HR, IT manager
Distribution of policy documents	HR	HR Director	Directors	All co-workers of Protime

Document control and revision history

Owner:	Protime IT
Effective as of:	1 October 2015
Approval:	Protime Directors
Last revision date:	14/02/2017

Revision History

Date	Author	Version	Changes
15/07/2015	Bart Slaets	1.0	Initial version
03/02/2017	Bart Slaets	1.1	Changed definition of 'Our websites'
14/02/2017	Bjorn Vanhevel	1.2	Add Internal IT ServerRoom Policy

Contact information

Technology Director @ Protime
Bart Slaets *
bart.slaets@protime.eu

* Representative of B-Inspired bvba