



# **SECURITY DOMAIN**

## Baltimore Certificates On-Line

SDPL –P08 (BC –PU) - Business Continuity Policy  
(Public)

---

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Security Domain Pty Limited.

Written and published in Sydney, Australia, by Security Domain Pty Limited.

Copyright © 1998 Security Domain Proprietary Limited,  
ACN 082 074 575.

All Rights Reserved.

---

## Table of Contents

Security Domain Pty Limited Business Continuity Policy (Public) .....	2
Introduction .....	2
Scope .....	2
Background .....	3
Service transition plan.....	4
SDPL obligations .....	4
CA Service obligations .....	5
Successor CA CPS <sub>(1)</sub> .....	6
Nominated successor CA .....	6

---

# SECURITY DOMAIN PTY LIMITED BUSINESS CONTINUITY POLICY (PUBLIC)

## Introduction

Good management practice demands the production and commissioning of various policies and plans.

In accordance with these requirements, Security Domain Pty Limited (SDPL) has prepared a Business Continuity Policy designated "Security Domain Pty Limited Business Continuity Policy (Public)", published below.

The purpose of this Policy is to ensure that in the event of the operational shutdown ("shutdown") of an element of the SDPL PKI hierarchy:

1. End Users' capacity to use Public Key Certificates is maintained; and,
2. the parties involved co-operate with each other in minimising any disruption that may be caused.

A copy of this document is published on the following website:

[www.secdom.com.au](http://www.secdom.com.au)

## Scope

This Policy covers the shutdown of:

1. Security Domain Pty Limited or the SDPL RCA;
2. the SDPL CA;
3. a Client CA within the SDPL PKI hierarchy;
4. the SDPL RA ;
5. a Client RA within the SDPL PKI hierarchy.

This Policy may be applicable to subordinate elements of the SDPL PKI hierarchy as described below.

**Security Domain Pty Limited or SDPL RCA**

In the event of a shutdown of Security Domain Pty Limited or the SDPL RCA, the provisions of this Policy shall apply to all service elements within the SDPL PKI hierarchy.

**SDPL CA**

In the event of a shutdown of the SDPL CA, the provisions of this Policy shall apply to all Branded Client CAs and their subordinate RAs.

**Client CA**

In the event of a shutdown of a Client CA (whether a Branded Client CA or an Externally Operated Client CA), the provisions of this Policy shall apply to that client CA and its subordinate RAs.

**SDPL RA**

In the event of a shutdown of the SDPL RA, the provisions of this Policy shall apply to any Branded Client CAs that may register their users through the SDPL RA.

**Client RA**

In the event of a shutdown of a Client RA, the provisions of this Policy shall apply to that client RA.

**Background**

SDPL has established this Policy to provide for a continuity of services in the event that SDPL ceases operations or a CA service within the SDPL PKI hierarchy shuts down.

A shutdown of SDPL or a SDPL PKI service element may be programmed or non programmed, as described below.

**Programmed shutdown**

A programmed shutdown is any event where:

1. the shutdown of a CA service has been predetermined; and,
2. the shutdown has been planned as a result of commercial decisions or corporate strategies; and,

3. the circumstances surrounding the shutdown allow a minimum of three month's notice to be given to subordinate elements.

### **Non programmed shutdown**

A non programmed shutdown is any event where:

1. the shutdown of a CA service is unanticipated; and,
2. the shutdown occurs as a result of:
  - the exercising by SDPL or a client of provisions or prerogatives contained within a relevant contract or CPS<sub>(1)</sub>; or,
  - external circumstances; and,
3. the circumstances surrounding the shutdown allow less than three months' notice to be given to subordinate elements, including End Users.

## **Service transition plan**

Where a CA service is to be transferred to a nominated successor CA service, a detailed Service Transition Plan (STP) shall be established by the CA service with the assistance, as appropriate of SDPL. The STP shall provide for the orderly transfer of records and services to the replacement CA service.

The STP shall conform with the CA termination requirements of a relevant CPS<sub>(1)</sub> and CPS<sub>(2)</sub>.

An STP shall typically provide for:

1. timely notification to SDPL and End Users. In the case of a programmed shutdown, a minimum of three month's notice must be given;
2. the selection of an appropriate CA service or PKI hierarchy to take over the business operations of the terminating CA service;
3. the transfer of the terminating CA service's keys and Certificates to the replacement CA service in a manner agreed with SDPL (or in the case of a terminating RA, the transfer of RA records in adherence to the privacy principles set out in the Privacy Act);
4. the secure destruction of all private keys held by the terminating CA Service, that have been transferred to the replacement CA service;

## **SDPL obligations**

In the event of the shutdown of a CA service within the SDPL PKI, SDPL shall as appropriate:

1. authorise or endorse the shutdown; and,
2. provide clients with as much notice as is reasonable and practical, in the event of a programmed shutdown this shall be a minimum of three months' prior notice; and,
3. provide clients with the options of:
  - shutting down CA services to their End Users; or
  - self-certifying their operations through the establishment of their own RCA; or
  - sourcing an alternative service provider; and,
4. to whatever extent is reasonable and practical, assist clients who choose to continue to provide CA services to their End Users including:
  - the progressive transfer of CA services and operational records to a nominated successor CA service;
  - the preservation of any records not transferred to a successor CA, service including in need a transfer of records to the National Archives of Australia, or another nominated party.

## **CA Service obligations**

A terminating CA service shall:

1. establish an STP in terms of this document;
2. conform with the CA termination requirements of a relevant CPS<sup>(1)</sup> and CPS<sup>(2)</sup>.

## **End User certificates and keys**

In the event that a CA service shuts down:

1. all End User keys and certificates within the service's chain of trust may be revoked prior to the shutdown; or
2. all End User keys and certificates may be transferred to a replacement CA provided the certificates do not become operational within the chain of trust of the replacement CA service until after the shutdown of the terminating CA service; or

3. all End User certificates may be revoked prior to the shutdown of the terminating CA service and the End User keys may be transferred to the replacement CA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating CA service.

### **Successor CA CPS<sub>(1)</sub>**

The CPS<sub>(1)</sub> under which a nominated successor CA issues Certificates is a contractual matter between the client and the successor CA. In principle, however, to the extent that it is practical and reasonable:

1. the successor CA should assume the same rights, obligations and duties as the terminating CA;
2. the CPS<sub>(1)</sub> under which the successor CA issues Certificates should impose the same requirements and confer the same benefits as the CPS<sub>(1)</sub> under which the terminating CA issued Certificates;
3. the successor CA should agree to issue new Certificates to every End User whose Certificates were revoked due to the shutdown of the terminating CA, but only where the End User applies for a new Certificate and satisfies the CPS<sub>(1)</sub> initial registration and identification requirements.

### **Nominated successor CA**

In the event that an externally operated client CA shuts down and the client chooses to continue to provide CA services to their end users, the nominated successor CA shall be the SDPL CA, unless otherwise specified in a relevant CPS<sub>(1)</sub>.