Quick Guide for Use and Control of Electronic Records for Statutory Compliance

This Quick Guide provides a short overview of the requirements necessary for Electronic Records Systems that provide compliance evidence in the form of records for statutory authorities.

Issue Date: 10th February 2004

Version: Draft 00.2

This document is part of a set of three documents:

1. Quick Guide for Use and Control of Electronic Records for Statutory Compliance
2. Guidelines on the Use and Control of Electronic Records for Statutory Compliance
3. Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist

Preamble

There are many different types of information collected, processed and recorded during the various activities undertake by companies. Much of this information is used by companies to make decisions, to record transactions and generate reports for internal and external use.

There is one special type of information that is generated within certain companies that has an importance outside of the company. This is the information that is used for statutory compliance records. These special statutory compliance records have certain legal obligation in relation to the activities of the company and the representation of the business to the greater community including the countries to which Australia exports products.

These statutory compliance records have traditionally been paper based with a signature by the authorised company representative. These signed paper records formed the basis of legal evidence of the activities of the company. These paper records could be audited and readily transported, inspected, checked, verified and referenced.

With the advent of electronic records systems these simple principles have changed. Electronic records systems have been in use for many years by many companies. The difference is that electronic records systems are now being used for statutory compliance records. Where records are for internal business use the electronic records systems only had to satisfy the demands of the company. When used for statutory compliance records these electronic records systems must meet the legislative requirements that support the statutory compliance process.

Companies must be able to vouch for the reliability of the records upon which statutory compliance decisions are made, or actions taken.

To help companies and software developers to understand the complex requirements of statutory compliance records a series of documents have been prepared.

The series is made up of the following three documents:

1. Quick Guide for Use and Control of Electronic Records for Statutory Compliance
2. Guidelines on the Use and Control of Electronic Records for Statutory Compliance
3. Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist

Each document is intended to provide assistance at a different level of a company.

The first document, "Quick Guide for Use and Control of Electronic Records for Statutory Compliance" is the current document you are reading. The document is a short document that outlines the principles and issues that must be followed.

The second document, "Guidelines on the Use and Control of Electronic Records for Statutory Compliance" is a detailed comprehensive explanation of the issues that must be addressed.

The third document, "Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist", is a check list that can be used by companies to measure their respective level of compliance to the guidelines.

There are a number of principles that must be addressed for the successful design, implementation and maintenance of Electronic Records Systems for statutory compliance. These issues have been summarised as:

1. Management of the Company's Electronic Records System

- A senior member of the Company must have clear responsibility for all aspects of the Electronic Records System. The Electronic Records System Management Representative could be the QA Manager or the IT Manager.

- The Electronic Records System Management Representative must ensure that Policies and Standard Operating Procedures are developed, approved, implemented and maintained for the following:
  - Electronic information risk assessment and management plan;
  - Management responsibility for electronic information;
  - Electronic information access and authenticity (user access, electronic signatures, database date time snapshots, date time stamps and off site 3rd party archiving);
  - Creation, maintenance, availability, access, archive, retrieval and destruction of electronic information;
  - Physical security of electronic information systems and data;
  - Electronic security (networks, email, viruses, internal and external) of electronic information;
  - Personnel security (user authenticity, access levels, maintenance and identification);
  - Disaster planning, management and recovery related to electronic information;
  - Personnel training in electronic information management;
  - Incident identification, reporting and response; and
  - Internal and external audit of electronic information;

2. The Company critical information that is recorded electronically and is related to statutory compliance is managed in a defined and controlled manner, that includes:

- Determining and documenting in a controlled manner what information is required for statutory compliance;

- Determining and documenting in a controlled manner when this information created and how often;

- Determining a method to create a unique and encrypted electronic record (collection of information or data related to a single or group of evidence, transactions, observations or similar instances), that includes:
  - A Unique identification for the electronic record;
  - Identifying the authors both as an organisation and the individual;
  - Establishing the time and date of the creation;
  - Establishing a system for alteration recording and reporting;
  - Establishing a system for authenticity (by approved encryption methods) of the electronic record;
  - Establishing a system for sending statutory specified electronic records to nominated third parties for independent back up; and
  - Establishing the reliability of the computer system that created, maintained, reported and moved the electronic records (through audit, testing and independent expert validation);

3. Statutory authority responsible for compliance approval of the Company's Electronic Records System - Management System (Policies and Standard Operating Procedures) .

Reference Documents

The three "Use and Control of Electronic Records for Statutory Compliance" documents are based on the following Australia Standards:

- HB 171-2003 Guidelines for the Management of IT Evidence
- AS ISO 15489.1-2002 Records Management Part 1: General
- AS ISO 15489.2-2002 Records Management Part 1: Guidelines
- AS/NZS 7799.2:2003 Information Security Management Part 2
- AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management

The acts that have been identified as applicable to the statutory compliance requirements include the following:

- Electronic Transaction Act 1999 (Commonwealth)
- Electronic Funds Transfer Code of Conduct (National Scheme)
- Electronic Transactions (Victoria) Act 2000 (VIC)
- Electronic Transactions Act 2000 (TAS)
- Electronic Transactions Act 2000 (NSW)
- Electronic Transactions Act 2000 (SA)
- Electronic Transactions (Queensland) Act 2001 (QLD)
- Electronic Transactions Act 2001 (ACT)
- Privacy Act 1988 (Cth)
- Privacy Amendment (Private Sector) Act 2000 (Cth)