



SecureWave
Safeguarding Tomorrow



Sanctuary Device & Application Control BS7799 Compliance



Table of Contents

1	About this document.....	3
1.1	Context	3
1.2	Purpose.....	3
1.3	Scope.....	3
1.4	Definitions & Acronyms.....	3
1.5	Document history	4
2	Introductions.....	5
2.1	BS 7799 Background	5
2.2	Sanctuary® Device Control.....	5
2.3	Sanctuary®	6
2.4	Architecture	8
3	Compliance	10



1 About this document

1.1 Context

To be read in conjunction with BS: ISO/IEC 17799:2000 (BS 7799-1:2000) which is available from British Standards Publishing Limited (BSPL): <http://www.bspl.com>

It is also important to consider that the necessity to implement a particular recommendation will be determined by the results of a formal risk analysis.

1.2 Purpose

To supply organisations considering the deployment of Sanctuary® Device Control and Sanctuary® with information concerning which sections of BS ISO/IEC 17799:2000 (BS 7799 - 1:2000) that they support.

1.3 Scope

Employees who are responsible for developing, implementing, and maintaining information security within their organisation.

1.4 Definitions & Acronyms

Terms	Definitions
ACL	Access Control List
AD	Active Directory
BSPL	British Standards Publishing Limited
CD	Compact Disc
DLL	Dynamic Link Library
I/O	Input/ Output
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
MS	Microsoft
MSI	Microsoft Installer
N/A	Not Applicable
NT	New Technology
OU	Organisational Unit
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adelman
SAC	<i>Sanctuary®</i>
SDC	<i>Sanctuary® Device Control</i>
SFD	SecureWave File Definition
SHA	Secure Hash Algorithm
SID	Security Identifier
SMC	SecureWave Management Console
TCP	Transmission Control Protocol
USB	Universal Serial Bus



1.5 Document history

Version	Date	Description	Author	Reviewer
1.0	12/1/2005	Completed compliance for review	P. Stewart	L. Oley
2.0	15/2/2005	Updates	P. Stewart	L. Oley



2 Introductions

2.1 BS 7799 Background

BS ISO/IEC 17799:2000 provides a comprehensive set of controls comprising best practices in information security. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organisations. The term organisation refers to both profit and non-profit making organisations, such as public sector organisations.

BS 7799:1-1999 was submitted as the proposed text for an international standard on Information Security Management using the ISO/IEC JTC 1 fast track procedure. During the resolution of comments phase of developments, it was agreed that the international standard would be considered as a single part standard until such time that further submissions/developments are produced.

For the purposes of implementation in the UK, the British standard has been dual numbered as:

BS ISO/IEC 17799:2000 *UK Implementation of the International Standard*

BS 7799-1:2000 *Retention of the original British Standard Identifier*

2.2 Sanctuary® Device Control

SecureWave extends the Windows Security model to centrally manage access to I/O devices at a user and/or group/ machine level within the windows domain.

All device access management and administration is done from one or more central, remote locations. It is not necessary to have physical access to a PC to set or change user permissions on that machine. Changes to user access can be granted "on the fly"; it is not necessary for the user to logoff or reboot for a device access permission change: they can be pushed down to the client PC if required.

Per-Device Permissions

In *Sanctuary® Device Control* there is the option of defining specific devices and assigning permissions to them. Rather than assigning permissions to all Removable media in exactly the same way, a specific device can be defined in *Sanctuary® Device Control* and permissions added to it instead. For example, if the corporate standard USB memory stick is a Disgo 32MB stick, it is possible to define that memory stick in *Sanctuary® Device Control* and assign group or user permissions to that device. Any other type of Removable media added will be denied access. In this way, it is possible to build up a White List of corporate-approved devices and deny everything else.

Per-User Permissions

Sanctuary® Device Control integrates with Microsoft's Certificate Services, making it possible to encrypt a removable device to a specific user. The data remains encrypted even if the device is plugged into another device where Sanctuary® Device Control is not installed. A simple decryption utility, combined with the ability to export the appropriate key allows the user to work with the device on a PC outside the user's organisation, e.g. home working.



Read-only Access

Sanctuary® Device Control makes it possible to set the access to a particular device to be read-only. This option is valid for all file-system based devices such as the floppy drive or PCMCIA hard drives. Read-only access on the CD-ROM drive, for example, prevents CD and DVD burning.

Scheduled & Temporary Access

Scheduled device access gives the option of granting or denying device access for a specific period of time and/or following a pre-defined schedule. This feature allows for the development of sophisticated security policies where certain devices can only be used from 9 to 5, Monday to Friday, for example.

Disk Authorization

In *Sanctuary® Device Control*, it is possible to grant specific user access to specific removable media/ external disks using the Disk Authorizer. For example, user A can access USB memory stick 1 but not 2 or 3; user B can access external disk 2 but not memory stick 1 or 3; user C can access USB memory stick 3 only. In this way an optional, additional level of security can be applied to writeable media.

Strong Audit Capability

SecureWave patent-pending I/O-shadowing allows you to track down information as it gets saved to Floppy, writable CD and DVD media and removable devices. Today, virtually all organizations keep track of what gets sent over email, but have no record of what gets saved over local I/O devices. Shadowing intercepts such operations. These shadowed file copies can then be viewed at a later stage by an authorized administrator.

I/O-shadowing also allows the logging of filenames only in order to offer a less intrusive way of monitoring file copies.

2.3 Sanctuary®

Sanctuary® is able to prevent against known and unknown (“zero day”) vulnerabilities. This is achieved by using the “White List” approach – allow only the known code within the organisation and deny all unknown code, preventing the execution of malware, Trojans, worms and spyware as well as unlicensed/ unauthorised applications. Recognition of executable code is based upon a unique digital signature using a SHA-1 algorithm, and not upon weaker attributes such as file location or extension. There is considerable flexibility in the product to accommodate dynamic and changing environments, using Non-blocking mode, Path Rules, Local Authorisation and Macro Protection.

Protection at all times

Sanctuary® affords organizations the same levels of control and protection regardless of whether the user or system is connected or isolated from the network. In standalone mode – when the client computer cannot communicate with the *Sanctuary®* Servers – it will consult its own database stored locally on the hard disk and consult the last list of authorized files. *Sanctuary®* will continue to use that list until it is able to connect to one of the *Sanctuary®* Servers to retrieve a later list.



Unlike the black list approach adopted by anti-virus technologies, *Sanctuary*[®] only allows authorised (known) code by identification by digital signature. Whether a threat is known or unknown is irrelevant to *Sanctuary*[®] – it is blocked. This prevents the execution of known malware; malware for which the corresponding AV update has yet to be developed; and vulnerabilities which are exploited immediately upon publication (“zero day vulnerability”). In each case, *Sanctuary*[®] will block their execution, since the hash generated for unknown code will not match that already known to the application (i.e. on the “White List”).

Prevents the installation of undesirable programs

Since *Sanctuary*[®] prevents the execution of unknown and undesirable applications, it also prevents their installation, as the installation program itself is an executable file, and therefore won't be permitted to run.

Effective Policy Support

Sanctuary[®] enables organizations to effectively deploy and manage their security policies regarding the installation and use of unauthorized software and the introduction and execution of malicious code.

File integrity checking

Sanctuary[®] works at the binary level. It thoroughly examines each executable that an administrator wishes to authorize and calculates a 20-byte unique digital signature using the SHA-1 algorithm based on the entire binary content of that executable. This digital signature is referred to as a hash. Any change made to an executable will result in a different hash and thus the file will not be allowed to run.

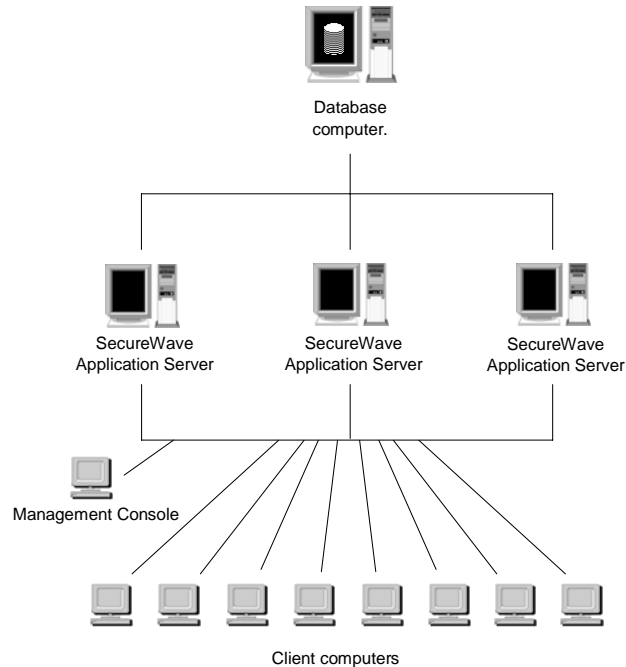
Increased productivity and stability

When *Sanctuary*[®] is deployed throughout the organization, it strongly reduces the required support and maintenance by improving the desktop and server environments stability and performance, and it lowers operational support costs without major process changes:

- > no user involvement needed.
- > no user work disruption.
- > easy deployment.
- > no continuous updates.
- > creates stability within the end user computing environment/experience.
- > reduces support operations costs.



2.4 Architecture



SecureWave's common architecture is presented in figure 1 above. The back-end is common to both *Sanctuary® Device Control* and *Sanctuary®*.

The architecture consists of 3 tiers of database, application server(s) and client driver, allowing the product to be scaled across a large enterprise and support thousands of users.

Database: The back end database is SQL Server (v 7.0 or 2000). MSDE is also supported for the purposes of evaluation. The database holds the user, computer and group SIDs which are extracted from the Active Directory at installation time (and subsequently replicated at client defined intervals using the `sxdomain.exe` utility). In addition, the digital signatures for all executable code (SHA-1 hashes) are stored in the database; along with the File Group information (a File Group is a collection of files which comprise an application, utility or component of the operation system). The SQL database also stores the logs concerning both user activity and *Sanctuary®* administrator actions.

Application Server(s): The purpose of the application server is act as a forwarder of requests from the client drivers to the database. They also optimise network traffic by performing a caching function at the application server level. In addition, the application server digitally signs client/ server communication using a public/ private key pair. In this way, a hacker or malicious user cannot spoof either an application server or client. The application server runs as an NT service.

Client: The clients (one for *Sanctuary® Device Control*; one for *Sanctuary®*) consist of kernel-level drivers. They intercept all requests for I/O device access/ application execution in memory, and checks whether the device/ code is authorised or not against a local cache. Running in kernel space means that the client is not visible to a user or administrator as a task or NT service, hence it is much more secure from hacking or tampering. Code that runs in kernel space is also more efficient than that in user space; hence there is no impact upon end user



performance in terms of either processor or memory utilisation on the client. In addition, it also means that local administrators are also subject to the enforced policy and are not exempt from the corporate policy. The client driver is packaged into an MSI file. It can easily be deployed using any MSI supported technology, or Microsoft Windows Group Policy.

SecureWave Management Console (SMC): The SecureWave Management consoles use RPC to communicate with a chosen application server. It can be installed on any machine in the enterprise (see Appendix B for minimum system requirements), and provides centralised, remote administration. From the SMCs the following operations can be performed:

- > Setting device access control policy
- > Defining a specific device or CD
- > Encrypting a device (removable media only)
- > Setting shadow file settings (file copy auditing)
- > Creating groups of files that are authorized to run.
- > Assigning executable files into manageable and logical file groups.
- > Granting permission to users to run files listed in the different file groups.
- > Setting options in the way the client computers operate using Sanctuary®.
- > Viewing execution logs.
- > Viewing device access logs
- > Viewing File Shadowing logs.
- > Viewing administrative audit logs.



3 Compliance

Below follows the list of **BS/ ISO IEC 17799: 2000** controls as outlined in Annex A of the BS7799-2:2002 standards document. The controls are up to date as of 12th January 2005. The control is listed, followed with the appropriate functionality in Sanctuary[®] Device Control/ Sanctuary[®] which assist towards meeting that control. Where either product does not have functionality relating to the listed control, "N/A" is listed. In some cases, additional procedures/ and or technologies may be required and thus the *BS ISO/IEC 17799:2000 (BS 7799 - 1:2000) Information Technology – Code of Practice for Information Security Management* document should be read in full in conjunction with this document, as well as a full risk analysis having been performed in determining an organisation's compliance to the standards.

BS/ ISO IEC 17799: 2000 Control	Control Description	Sanctuary [®] Device Control Functionality	Sanctuary [®] Functionality
A4.2.1	<p><i>Identification of risks from third-party access.</i></p> <p>The risks associated with access to organisational information processing facilities by third parties shall be accessed and appropriate security controls implemented</p>	Through the use of the Sanctuary [®] Device Console to control which users and/ or user groups have access to which devices, preventing unauthorised access by third party to organisational media stored on removable media when plugged in to a PC. In addition, removable media can be encrypted to protect it against unauthorised access should the device be lost/ stolen and plugged into a PC/ laptop external to the organisation.	Through the use of Sanctuary [®] , Custom Edition, access to applications is granted to only the authorised users and/ or user groups. Prevents access to sensitive material gained by opening unauthorised applications, which may or may not have internal password controls for application access. It is possible to identify which applications users are running, and applications which they have attempted to run but have been blocked by Sanctuary [®] .
A5.1.1	<p><i>Inventory of assets*.</i></p> <p>An inventory of all important assets associated with each information system shall be drawn up and maintained.</p> <p>* assets as defined in examples (a), (b) and parts of (c) only</p>	Sanctuary [®] Device Control can audit the use of unauthorised (and authorised) I/O devices and CDs by username, date and time.	Sanctuary [®] can audit the use of both authorised and unauthorised software across the enterprise, and by username, date and time.
A6.3.1	<p><i>Reporting Security Incidents.</i></p> <p>Security incidents</p>	In enforcing the procedure established in A6.3.1, Sanctuary [®] Device Control has in-built reporting which can be utilised	In enforcing the procedure established in A6.3.1, Sanctuary [®] has in-built reporting which can be utilised



	shall be reported through management channels as quickly as possible	to determine: <ul style="list-style-type: none"> • Which users are attempting to access unauthorised devices • Which users are copying data out of the organisation (and the amount) • Which I/O devices (by device type) have had data copied from them (and by whom, on which computer and amount) • What data is being copied out of the organisation (File Shadowing), either by file name or file name and content. It also indicates user, computer name and time of copy. 	to determine: <ul style="list-style-type: none"> • Which applications a user/ user group is running • Which denied applications a user/ group is attempting to execute • The number of times a particular application has been run (and by whom)
A6.3.3	<i>Reporting Software Malfunctions.</i> Procedures shall be established for reporting software malfunctions	N/A	Sanctuary® allows all software execution to be fully audited, indicating filename, username, computer name and time of execution
A6.3.4	<i>Learning from Incidents.</i> Mechanisms shall be put in place to enable the types, volumes and cost of incidents and malfunctions to be quantified and monitored	In Sanctuary® Device Control, File Shadowing allows audit capability of files copied out of an organisation and indicates file name or file name and content. Reporting of attempted (and successful) I/O device and CD access for unauthorised (or authorised) devices is also available. Thus date, times and the user(s) involved in incidents can easily be identified	Sanctuary® allows all software execution to be fully audited, indicating filename, username, computer name and time of execution. Thus date, times and the user(s) involved in incidents can easily be identified
A6.3.5	<i>Disciplinary Process.</i>	Sanctuary® Device Control prevents unauthorised access to an I/O device. For those users	Sanctuary® prevents unauthorised execution of applications. For users misusing



	The violation of organisational security policies and procedures by employees shall be dealt with through a formal disciplinary procedure.	misusing their authorised devices (such as for the purposes of data theft) then these events can be monitored and audited through the use of File Shadowing. Attempts to access an authorised device are also audited, and reported centrally to the SecureWave Management Console.	applications (attempting to run denied applications or using applications in an inappropriate way) then these events can be audited, and reported centrally to the Sanctuary® Console.
A7.1.1	<i>Physical Security Perimeters.</i> Organisations shall use security perimeters to protect areas that contain information processing facilities.	Sanctuary® Device Control prevents unauthorised access to an I/O device by an authorised user within the organisation. Using the Removable Media encryption, a removable media can be encrypted, using MS Certificate Services, and thus protect data on such a device from access by a user external to the organisation, should the device be lost or stolen.	N/A
A7.1.2	<i>Physical entry controls.</i> Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Sanctuary® Device Control prevents unauthorised I/O devices within the organisation from a PC or laptop. Encrypting a removable media device ensures that the data on the device is protected; when attempting to access the data outside of the organisation, both the key and the user password are required in order to access the encrypted data.	N/A
A7.1.4	<i>Working in Secure Areas.</i> Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.	Sanctuary® Device Control increases (and helps to enforce) network security by preventing unauthorised access to I/O devices from a PC or laptop.	Sanctuary® increases (and helps to enforce) network security by preventing unauthorised access to an application, and Trojan, worm, mass mailer viruses and spyware from executing.
A7.2.4	<i>Equipment Maintenance.</i> Equipment shall be correctly maintained	Sanctuary® Device Control improves PC and laptop stability by preventing unauthorised access to an I/O device or CD.	Sanctuary® improves PC, laptop, server and terminal server stability by preventing the execution of unauthorised code, such as viruses, Trojans,



	to enable its continued availability and integrity.		<p>worms, mass mailers, spyware and shareware.</p> <p>Network bandwidth (and hence server availability) is also improved by preventing the use of high bandwidth applications, such as Internet Radio, or zombie/ bot attacks.</p>
A7.2.6	<i>Secure disposal or re-use of equipment</i>	Sanctuary® Device Control allows a means of centralised management of access to I/O devices, including removable media. If removable media encryption is utilised, re-assignment of a device to a new user will require re- authorisation which can include the re-formatting of the device.	N/A
A7.3.2	<i>Removal of property.</i> Equipment, information, or software belonging to the organisation shall not be removed without authorisation of the management.	<p>Control of exactly which user groups and/or users is possible in Sanctuary® Device Control through the use of the Sanctuary® console. Granting/ revoking access to a user can be restricted to an administrator, who will have to seek management approval for the policy change. Thus device access is centrally controlled and information cannot be removed from the organisation onto an authorised device.</p> <p>In addition, removable media devices can be made "Read only", preventing transfer of data to them. For those devices which must be "Read/Write" , File Shadowing can audit the file name or file name and content of data copied to it.</p> <p>Devices can be encrypted using MS Certificate Services, assigning a specific device to a specific user or users, thus securing the</p>	Access to unauthorised business applications which may contain sensitive data (e.g. payroll processing systems) can be prevented using Sanctuary® through the console to either a user group and/ or user.



		<p>data, even when the device is used outside the organisation where Sanctuary® Device Control client is not loaded.</p> <p>Unauthorised CD access can be prevented using the "Media Authoriser", where it is possible to restrict access to a specific CD to a specific user and/or or group, if so required.</p>	
A8.1.3	<p><i>Incident Management Procedures.</i></p> <p>Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs.</p>	<p>Sanctuary® Device Control provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) I/O device access, indicating the user, date and time of access • CD access, indicating the CD (as registered to SDC), user, date and time of access • If File Shadowing is enabled, the file name or file name and content of files copied from a PC or laptop to a writeable device (removable media, CD, floppy diskette) • If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto writeable media by user, indicating username, computer name, device type and amount of data copied within a chosen timeframe. • If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto 	<p>Sanctuary® provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) attempted access to application executions, indicating username, computer name, date and time of (attempted) execution • The number of times a selected file has been run, including username, computer name, date and time of (attempted) execution



		writeable media by device type, indicating username, computer name and amount of data copied within a chosen timeframe.	
A8.1.4	<p><i>Segregation of Duties</i></p> <p>Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorised modification or misuse of information and services.</p>	<p>Sanctuary® Device Control Console supports AD delegation. Administrators of a site or domain in the AD forest will only be able to view the corresponding objects in the Sanctuary® Device Console for which they have administrative rights.</p> <p>In addition, it is possible to restrict access to particular parts of the console for a given user, such as: audit view only; and/or shadow-file review only; and/or device management settings only.</p> <p>The use of Sanctuary® Device Control can provide different levels of I/O device access for different users/ groups of users. Thus it is easy to correlate job role based on AD/ NT 4.0 user group, and then assign the appropriate I/O device access for that group in the Sanctuary® Device Console.</p>	<p>Sanctuary® Console supports AD delegation. Administrators of a site or domain in the AD forest will only be able to view the corresponding objects in the Sanctuary® Device Console for which they have administrative rights.</p> <p>In addition, it is possible to restrict access to particular parts of the console for a given user, such as: audit view only; and/or execution log settings view only; and/or machine scans only; and/or application control settings.</p> <p>The use of Sanctuary® can provide different levels of application authorisation for different users. Thus it is easy to correlate job role based on AD/ NT 4.0 user group, and then authorise the appropriate application to that group in the Sanctuary® Console.</p>
A8.1.5	<p><i>Separation of development and operational facilities.</i></p> <p>Development and testing facilities shall be separated from operational facilities. Rules for the migration of software from development to operational status shall be defined and documented.</p>	<p>Sanctuary® Device Control assists in the separation of development and operational facilities by preventing access to unauthorised (un-tested) devices on the operational platform.</p>	<p>Sanctuary® prevents the execution of unauthorised code in the operational environment.</p> <p>In the development and testing environment, trial code can be permitted to run by using Local Authorisation, an option to allow users to self-authorise their own software that is not on the centrally-authorised white list. This affords protection against malware and spyware, whilst allowing developers and testers to perform their duties.</p>



			The hashes for code scanned and authorised on the testing environment can be exported to the operational environment using the fimpex utility.
A8.3.1	<p><i>Controls against malicious software</i></p> <p>Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.</p>	Sanctuary® Device Control prevents the use of unauthorised devices, and thus the introduction of potential malware, spyware and other harmful code into the organisation.	Sanctuary® prevents the execution of unauthorised code using a SHA-1 algorithm. This renders malware, spyware and execution viruses ineffective, as no code will run unless it is on the approved, centrally authorised "white list".
A8.4.2	<p><i>Operator Logs.</i></p> <p>Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.</p>	Sanctuary® Device Control provides an audit log of Sanctuary® administrator actions, including: granting/revoking access to a device for a user or group; defining a new device; accessing log files and shadow files. Thus administrative changes to I/O device access policy can be tracked.	Sanctuary® provides an audit log of Sanctuary® administrator actions, including: authorising/removing an application to a user or group; approving a file into the whitelist; accessing log files. Thus administrative changes to application policy can be tracked.
A8.5.1	<p><i>Network controls.</i></p> <p>A range of controls shall be implemented to achieve and maintain security in networks</p>	Sanctuary® Device Control provides control of unauthorised I/O devices, thus establishing the perimeter at the device level.	Sanctuary® prevents the execution of unauthorised code on the network, and the use of unauthorised, high bandwidth applications such as streaming media and Internet Radio. Exploits such as Ping of Death and mass mailer viruses are prevented from execution, network integrity and bandwidth.
A8.7.2	<p><i>Security of media in transit</i></p> <p>Media being transported shall be protected from unauthorised access, misuse or corruption</p>	Sanctuary® Device Control integrates with MS Certificate Services to encrypt removable media at a user level. The data is encrypted and accessible only to the designated user(s). If the device is connected to a PC or laptop where the Sanctuary® Device Control client driver is not installed, the data will be	N/A



		inaccessible.	
A8.7.3	<p><i>Electronic commerce security.</i></p> <p>Electronic commerce shall be protected against fraudulent activity, contract dispute, and disclosure or modification of information.</p>	<p>Sanctuary® Device Control prevents unauthorised access to I/O devices and thus data stored on them. Only the authorised users can access an authorised device using the "Removable Media manager". This encrypts the devices using MS Certificate Services, thus ensuring the data contained on it is not compromised or able to be modified except by the authorised user(s).</p> <p>In addition, File Shadowing allows an audit to be taken of the file name (and optionally content as well) of any file copied by a user onto a writeable I/O device (examples: floppy, digital camera, USB pen), thus ensuring that users are not abusing their device access and copying out confidential information.</p> <p>A user daily transfer limit specifies a daily user quota of the amount of data that a user can copy out of the organisation onto removable media. Thus, if a 2GB USB memory key is authorised to a user, a user daily transfer limit of 50MB will allow them to perform their day to day duties but will prevent the copying of a 1GB corporate database onto the pen.</p>	Sanctuary® prevents unauthorised access to applications, both unauthorised business applications and malware.
A8.7.4	<p><i>Security of electronic mail.</i></p> <p>A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.</p>	N/A	Sanctuary® blocks all execution of execution based mail attachments, thus preventing mail-borne viruses. If the "Macro Protection" feature is enabled, all script and macros will be subject to user checking prior to execution, removing another mail-based threat.
A9.1.1	<p><i>Access Control Policy.</i></p> <p>Business</p>	The use of Sanctuary® Device Control enables a device control	The use of Sanctuary® enables an application usage policy to



	requirements for access controls shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	access policy to be defined and enforced. The in-built reports, which can be printed or saved electronically, allow the Sanctuary® administrator to list current device access policy.	be defined and enforced. The in-built reports, which can be printed or saved electronically, allow the Sanctuary® administrator to list current application access policy.
A9.2.2	<i>Privilege Management</i> The allocation and use of privileges shall be restricted and controlled.	Access to the Sanctuary® Device Console can be restricted to a specific user group or user. In addition, each Sanctuary® administrator can have: audit view only; and/or shadow-file review only; and/or device management settings access.	Access to the Sanctuary® Console can be restricted to a specific user group or user. In addition, each Sanctuary® administrator can have: audit view only; and/or execution log settings view only; and/or machine scans only; and/or application control access.
A9.2.4	<i>Review of user access rights.</i> Management shall conduct a formal process at regular intervals to review user's access rights	Sanctuary® Device Control provides extensive user auditing which provides for I/O device access (unauthorised attempts and authorised usage); file copying (file name or file name and content); and CD access.	Sanctuary® provides extensive user auditing which provides for application usage (attempted execution of unauthorised applications; application execution).
A9.4.1	<i>Policy on the use of network services</i> User shall only have direct access to the services that they have been specifically authorised to use.	N/A	Sanctuary® authorises a specific application or service to a specific user or user group. Thus it ensures that users can only run the network services they are authorised to use.
A9.4.6	<i>Segregation in networks</i> Controls shall be introduced in networks to segregate groups of information services, users and information systems.	Sanctuary® Device Control prevents access to unauthorised I/O devices on the network. Those devices which are not explicitly authorised by device type (make and model) or explicit device (encrypted, using MS Certificate Services) cannot be accessed by an authorised user. This assists in segregating user access to devices used only in testing or development to which access would not be appropriate for an operational environment. Similarly, those users whose job	Sanctuary® provides the capability to control which applications can be executed by which users based upon Windows' security group or user. Thus it can be used to fully segregate services and users as required. As recognition is based upon file hash, and not weaker attributes such as file name or extension, different versions of the same application can be



		functions entail using sensitive data (e.g. finance, HR) can use these features of Sanctuary® Device Control to ensure these devices cannot be accessed by unauthorised users.	assigned to different users.
A9.5.5	<p><i>Use of system utilities.</i></p> <p>Use of system utility programs shall be restricted and tightly controlled.</p>	N/A	Sanctuary® can be utilised to restrict system utilities (pre-configured in a File Group called "Administration Tools") to only the desired user(s) or group (e.g. "Domain Admins")
A9.6.1	<p><i>Information access restriction.</i></p> <p>Access to information and application system functions shall be restricted in accordance with the access control policy.</p>	Sanctuary® Device Control prevents the unauthorised use of devices containing sensitive material using "per-user" permissions. This is achieved by integration with MS Certificate Services, where the device is encrypted and authorised to one or more user(s) as specified in the Sanctuary® Device Console.	Sanctuary® prevents the unauthorised use of applications which may contain sensitive information which is restricted/ sensitive.
A9.6.2	<p><i>Sensitive System isolation.</i></p> <p>Sensitive systems shall have a dedicated (isolated) computing environment.</p>	Sanctuary® Device Control assists in the setting up of an isolated environment, by preventing unauthorised user access to I/O devices and assigning a specific user(s) to a specific removable media device.	N/A
A9.7.1	<p><i>Event Logging</i></p> <p>Audit logs recording exceptions and other security-related events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.</p>	<p>Sanctuary® Device Control provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) I/O device access, indicating the user, date and time of access • CD access, indicating the CD (as registered to SDC), user, date and time of access • If File Shadowing is enabled, the file name or file name and content of files copied from a PC or laptop to a writeable 	<p>Sanctuary® provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) attempted access to application executions, indicating username, computer name, date and time of (attempted) execution • The number of times a selected file has been run, including username, computer name, date and time of (attempted) execution



		<p>device (removable media, CD, floppy diskette)</p> <ul style="list-style-type: none"> If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto writeable media by user, indicating username, computer name, device type and amount of data copied within a chosen timeframe. <p>If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto writeable media by device type, indicating username, computer name and amount of data copied within a chosen timeframe.</p>	
A9.7.2	<p><i>Monitoring system use.</i></p> <p>Procedures for monitoring the use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.</p>	As for A9.7.1 above	As for A9.7.1 above
A9.8.1	<p><i>Mobile Computing</i></p> <p>A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.</p>	<p>Sanctuary® Device Control prevents unauthorised user access to I/O devices and allows a policy to be put in place regarding device access, based on user group and/or user.</p> <p>Users working remotely on laptops will not be able to access devices used in the home working environment, which would otherwise compromise the network security perimeter by introducing spyware, malware or data infected with a virus, Trojan or worm.</p>	Sanctuary® prevents unauthorised execution of an application, which has not been pre-authorised on a whitelist. This combats the problems of mobile working, where a traditional AV signature is not updated for many days or weeks at a time as the laptop is not on the corporate network to receive updates; the laptop then becomes infected with viruses and when the laptop is returned to the corporate network, it infects the network with the virus. With Sanctuary® installed, unauthorised code



			cannot run and thus laptops no longer act as a weak point in perimeter defences.
A10.3.2	<p><i>Encryption</i></p> <p>Encryption shall be applied to protect the confidentiality of sensitive or critical information</p>	Sanctuary® Device Control integrates with MS Certificate Services to allow encryption of removable media. Such media can then only be accessed by the authorised user(s). The data remains encrypted, even if the device is plugged into a PC not protected by Sanctuary® Device Control.	N/A
A10.4.1	<p><i>Control of operational software.</i></p> <p>Procedures shall be in place to control the implementation of software on operational systems</p>	In Sanctuary® Device Control, it is possible to define a CD (based upon the CD header, recognised via an SDC generated hash) via the console. Once defined, it is possible to authorise the CD via the "Media Authoriser" to either a user group or specific user. For example, a software upgrade performed by a third-party could be controlled. The user group "installers" could be restricted only to use the upgrade CD, thus ensuring that only the correct operational software is deployed, where CD is necessary.	In Sanctuary®, users who are authorised to install applications can be determined by authorising the "setup" file group to the appropriate user group or user(s). Thus only authorised users can be allowed to perform application installations.
A10.4.3	<p><i>Access control to program source library.</i></p> <p>Strict control shall be maintained over access to program source libraries.</p>	N/A	Sanctuary® allows the authorisation of specific applications to specific users. Thus, all developer applications can be authorised only to the appropriate user(s)/ user group, as required.
A10.5.3	<p><i>Restrictions on changes to software packages.</i></p> <p>Modifications to software packages shall be discouraged and essential changes strictly controlled.</p>	N/A	Sanctuary® permits only those applications to execute which have been pre-defined on the authorised whitelist. Modified code will not run, since the digital hash the client driver will produce for the modified code will not match the hash for the original code. In this way, it is easy to enforce a centralised approach to



			software changes and control. Software packages which are updated and approved for use can easily be added to the whitelist, using the "Authorisation Wizard", which will extract any .MSI, .CAB, or .ZIP file, in addition to scanning CDs.
A10.5.4	<p><i>Covert channels and Trojan code</i></p> <p>The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and Trojan code.</p>	N/A	Sanctuary® allows only the execution of code on a pre-defined whitelist. Code not on the whitelist cannot execute. Recognition of code is based upon a highly secure SHA-1 algorithm, and not weaker attributes such as file name, location or extension. This prevents the execution of all malware, both known and unknown threats including: Trojans, worms, viruses, spyware, and "zero-day" attacks.
A10.5.5	<p><i>Outsourced software development.</i></p> <p>Controls shall be applied to secure outsourced software development.</p>	N/A	Applications are restricted to specific users and/or groups. Third-party developers can thus be prevented from access to unsuitable applications/ services as required.
A11.1.1	<p><i>Business continuity management process.</i></p> <p>There shall be a managed process in place for developing and maintaining business continuity throughout the organisation.</p>	The use of Sanctuary® Device Control increases desktop and laptop stability (and thus availability) by preventing user access to unauthorised devices.	The use of Sanctuary® increases desktop, laptop and server (Citrix, Windows TS, file, print, application, mail server) by preventing the execution of unauthorised applications and malware, spyware, Trojans and worms. Thus stability and availability are increased, as is user productivity.
A12.1.2	<p><i>Intellectual property rights (IPR)</i></p> <p>Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of</p>	Using Sanctuary® Device Control and MS Certificate Services, allows a specific removable media to be encrypted, and only accessible to those user(s) specified in the "User to Media" applet in the console. Thus sensitive data is protected in	Sanctuary® ensures that only users authorised to use a specific application can do so. Thus, if used with the use of AD/ NT 4.0 groups then a specific user group (e.g. "Office 2003 users") can be authorised to use a specific application (Office



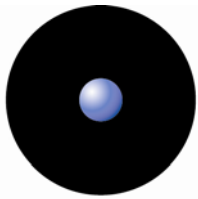
	material in respect of intellectual property rights, and on the use of propriety software products.	when stored on removable media, such as a USB memory pen.	2003 suite) so that licensing is maintained. In addition, users attempting to access applications unauthorised to them will be denied, thus preventing access to sensitive information.
A12.1.3	<p><i>Safeguarding of organisational records.</i></p> <p>Important records of an organisation shall be protected from loss, destruction or falsification.</p>	With the encryption feature of Sanctuary® Device Control, sensitive data stored on removable media can be encrypted. If the device is lost, stolen then the unauthorised user will not be able to access the encrypted data.	Access to unauthorised applications is prohibited, preventing inadvertent/ malicious access to unauthorised records.
A12.1.4	<p><i>Data protection and privacy of personal information.</i></p> <p>Controls shall be applied to protect personal information in accordance with relevant legislation.</p>	As for A12.13 above	As for A12.13 above
A12.1.5	<p><i>Prevention of misuse of information processing facilities.</i></p> <p>Management shall authorise the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities</p>	Authorised I/O devices and only allowed within the organisation. Access to devices can be defined based upon the device class (e.g. Removable media, CD, floppy, etc.) or device (make and model, e.g. Disgo 128MB memory key)	Access to only the authorised applications on the white list is permitted: access to unauthorised applications is denied.
A12.1.7	<p><i>Collection of evidence.</i></p> <p>Where action against a person or organisation involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the</p>	<p>Sanctuary® Device Control provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) I/O device access, indicating the user, date and time of access • CD access, indicating the CD (as registered to SDC), user, date and time of access 	<p>Sanctuary® provides an audit and log of the following:</p> <ul style="list-style-type: none"> • Unauthorised (and authorised) attempted access to application executions, indicating username, computer name, date and time of (attempted) execution • The number of times a selected file has been run, including



	<p>specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence.</p>	<ul style="list-style-type: none"> • If File Shadowing is enabled, the file name or file name and content of files copied from a PC or laptop to a writeable device (removable media, CD, floppy diskette) • If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto writeable media by user, indicating username, computer name, device type and amount of data copied within a chosen timeframe. <p>If File Shadowing is enabled, a report on the amount of data being copied out of the organisation onto writeable media by device type, indicating username, computer name and amount of data copied within a chosen timeframe.</p>	<p>username, computer name, date and time of (attempted) execution</p>
A12.2.2	<p><i>Compliance with security policy.</i></p> <p>Managers shall take action to ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organisation shall be subject to regular review to ensure compliance with security policies and standards.</p>	<p>All previous sections are relevant</p>	<p>All previous sections are relevant</p>
A12.2.3	<p><i>Technical compliance checking.</i></p> <p>Information systems shall be regularly checked for</p>	<p>See 12.1.7 above</p>	<p>See 12.1.7 above</p>



	compliance with security implementation standards.		
A12.3.1	<p><i>System audit controls.</i></p> <p>Audits of operational systems shall be planned carefully and agreed to minimise the risk of disruptions to business processes</p>	<p>The auditing of user I/O device access and file copying (File Shadowing) can be implemented/ disabled on the fly and is transparent to the end user. All auditing, except for "File name & content" File shadowing, does not provide a burden upon the network in terms of data uploaded from the client to the SecureWave Application Server.</p> <p>"File name & Content" File shadowing produces a like for like overhead, e.g. 10MB copied produces 10MB uploaded, and thus is used on a per-machine basis to investigate misuse of file copying.</p>	<p>The auditing of user application access (and attempts) can be implemented/ disabled on the fly and is transparent to the end user. It does not provide either performance degradation on the client machine, or a large burden upon the network in terms of the data uploaded from the client to the SecureWave Application Server.</p>
A12.3.2	<p><i>Protection of system audit tools.</i></p> <p>Access to system audit tools shall be protected to prevent any possible misuse or compromise.</p>	<p>It is possible to restrict access to particular parts of the console for a given user, such as: audit view only; and/or shadow-file review only; and/or device management settings only.</p>	<p>It is possible to restrict access to particular parts of the console for a given user, such as: audit view only; and/or execution log settings view only; and/or machine scans only; and/or application control settings.</p>



SecureWave

Safeguarding Tomorrow

North America

2325 Dulles Corner Blvd.
Suite 500, #8
Herndon, VA 20171
United States of America

+1 (703) 788-6760 Phone
+1 (703) 788-6511 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom

+44 (0) 1908 357897 Phone
+44 (0) 1908 357600 Fax

Continental Europe

Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Grand Duchy of Luxembourg

+352 265 364-11 Phone
+352 265 364-12 Fax

www.securewave.com
info@securewave.com