Blancco Drive Eraser Certified for Government Use in Australia and New Zealand

Australasian Agencies Have Additional Protection Against Unauthorised Data Access

Government data and asset managers in Australia and New Zealand can now confidently use Blancco Drive Eraser (BDE) to sanitise end-of-life data from loose hard disk drives and solid-state drives, as well as those in PCs, laptops and servers.

In June of 2020, the Australasian Certification Authority (ACA) awarded BDE 6.9.1 Common Criteria (CC) certification via its Australasian Information Security Evaluation Program (AISEP). This assures government users that Blancco Drive Eraser has met evaluation criteria recognised by all members of the Common Criteria Recognition Arrangement (CCRA), including Australia and New Zealand.

This is good news for agencies that adhere to data sanitisation requirements within

- the Australian Government Information Security Manual (ISM),
- the Australian Privacy Principles guidelines (APP) 11.2,
- the New Zealand Information Security Manual (NZISM),
- the New Zealand Privacy Act (1993) and
- other mandates regarding data erasure, such as the GDPR's data minimisation and 'right to be forgotten' articles.

The Common Criteria certificate is valid for five years from the award date unless it is renewed.

Common Criteria Certification and the EPL

In the past, the Australian Cyber Security Centre (ACSC) posted CC-certified products on its Evaluated Products List (EPL). Recently, however, the ACSC decided to list AISEP's Common Criteria-certified products only on the Common Criteria Portal's Certified Products List (CPL). This decision provides a 'single point of truth' for ACSC CC-certified products and affirms government use of CPL products.

NOTE: Products listed on the Common Criteria Portal's Certified Products list are considered Evaluated Products for purposes of the ISM. The Common Criteria Mutual Recognition Arrangement means these products are recognised at the EAL2 level, or against the relevant appropriate Protection Profiles of their evaluation. These products do not need to be dual listed on the EPL.

Blancco Driver Eraser and the Common Criteria Evaluation

Why is the Common Criteria certification important to Australasian government organisations?

Common Criteria is an internationally recognised standard (ISO 15408) for evaluating information and communications technology security products. The Common Criteria Recognition Arrangement is an international arrangement that recognises CC-certified products among its 31 member nations after rigorous evaluation by independent, licensed laboratories. These government licensed laboratories adhere to specified criteria and assessment methods to evaluate the security properties of a security product.

The standardised examination includes software architecture, safety precautions, customer delivery practices and more. Certification therefore provides government users with a level of assurance that the product is well engineered and does what it says it will do. It also provides product users with the assurance that the product can withstand various threats when used in accordance with the certificate's noted Evaluation Assurance Level (EAL).

Certifications up to EAL2 are recognised by all nations involved in the CCRA, including Australia and New Zealand, depending on national procurement policies. For media sanitisation products, Blancco Drive Eraser 6.9.1 was evaluated and certified to EAL2, which aligned with the CCRA mutual recognition.

The independent testing laboratory evaluated Blancco Drive Eraser on several erasure algorithms, or recognised standards, as well as several security mechanisms. It also evaluated the product's ability to manage erasures locally and remotely from the Blancco Management Console (BMC). Evaluators assessed the soundness of the product's development and delivery practices, as well as countermeasures against tampering, such as secure communication protocols, data encryption and key management. The goal was to test against security functions that would be important to BDE users while providing an accurate representation of Blancco's product and engineering capabilities.

> Blancco Drive Eraser is software that is used to securely erase information from various persistent store technologies including traditional hard disk drives (HDDs) and newer solid state drives (SSDs)...
>
> There are many algorithms for erasing data drive information. Blancco Drive Eraser supports proprietary and standard algorithms that can be selected as required by the user... Another important function performed by the [Target of Evaluation] is the generation of reports that are protected from tampering—thus providing a valuable record of data drive erasure activities performed by the user.
>
> —AISEP Certification Report for Blancco Driver Eraser v6.9.1, p. 7

Blancco Drive Erasure Offers Robust Compliance & Added Efficiency for Australia's Public Sector

With the flexibility to address everything from loose drives in data centres, to various types of HDDs, to new and more complicated SSDs (including NVMes) and ATA self-encrypting drives, Blancco Drive Eraser is customisable to address government agencies' varied erasure needs:

- Blancco Drive Eraser satisfies relevant sanitisation specifications set out by the Australian ISM, NZISM, Australian Privacy Principles guidelines 1 and 11 and the NZ Privacy Act.
- It ensures that sensitive data has been sanitised from servers, laptops, desktops and drives, verifying each step in the erasure procedure.
- It provides a digitally signed, tamper-proof certificate to prove compliance for each erasure procedure.
- It sanitises to more than 25 internationally recognised standards, including NIST 800-88 Clear and Purge, HMG InfoSec Standard No: 5 Higher and Lower standards, BSI-GS/GSE and more.

Government agencies also benefit from BDE's scalability to create added efficiencies and optimise staff time. For instance, with Blancco Drive Eraser, you can:

- Fully automate the erasure process across on-premise or remote environments
- Automate the hard drive erasure process to remove BIOS freeze locks
- Sanitise data permanently from multiple drives simultaneously
- Standardise and automate data sanitisation policies
- Receive the full audit trail to prove compliance with data privacy regulations

Because data erasure leaves working assets intact and functional, Blancco Drive Eraser supports fiscally responsible device reuse and environmentally friendly recycling—all with the peace of mind that sensitive data has been rendered irretrievable.

Blancco Drive Eraser, Data Sanitisation & ISM Guidelines

The ACSC Certification Report recommends that government users refer to their respective security manuals.

The following is a sample of Australian Government ISM guidelines for media sanitisation under the section, 'Guidelines for Media Management,' that are fulfilled by Blancco Drive Eraser 6.9.1:

ISM GUIDELINE	HOW BLANCCO HELPS
Media in ICT equipment 'ICT equipment will often contain devices that are quite small and may not be immediately recognisable as memory. Examples of these include M.2 or Mini-Serial Advanced Technology Attachment (mSATA) devices. When sanitising M.2 or mSATA devices, the methods for flash memory devices apply. Generally, if a device offers persistent storage of information, it is likely that the methods for flash memory will apply.'	Blancco Drive Eraser can detect and sanitise drives including SSDs with the M.2 form factor through overwriting and, if supported, firmware erasure. It also can sanitise mSATA devices.
Solid-state drives 'When sanitising solid-state drives (SSDs), the methods for flash memory devices apply.'	Blancco Drive Eraser sanitises all data storage devices, from HDDs and standard SSDs to NVMes with our patented erasure method. Blancco's secure erasure methods ensure data is written across the full logical capacity of the drive (and not just compressed). Blancco's multi-phase, proprietary SSD erasure (Patent No. 9286231) approach utilises all supported SSD security protocols. This innovative method includes multiple random overwrites, firmware level erasure, freeze lock removal and full verification.
Non-volatile flash memory media sanitisation 'In flash memory media, a technique known as wear levelling ensures that writes are distributed evenly across each memory block. This feature necessitates flash memory being overwritten with a random pattern twice as this helps ensure that all memory blocks are overwritten.'	In both magnetic and SSD drives, Blancco Drive Eraser offers overprovisioning to handle wear levelling. This guarantees 100% data sanitisation and is backed by a tamper-proof report. Blancco's multi-phase, proprietary SSD erasure (Patent No. 9286231) approach utilises all supported SSD security protocols. This innovative method includes multiple random overwrites, firmware level erasure, freeze lock removal and full verification.
Media sanitisation process and procedures 'When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process was completed successfully.'	If required, Blancco Drive Eraser can be configured to verify that all sectors of the drive have been overwritten. BDE certifies every erasure with a tamper-proof report.
Non-volatile magnetic media sanitisation 'Both the host-protected area and device configuration overlay table of non-volatile magnetic media are normally not visible to an operating system or a computer's basic input/output system. Therefore, any sanitisation of the readable sectors of media will not overwrite these hidden sectors leaving any data contained in these locations untouched. Some sanitisation programs include the ability to reset media to their default state removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of media during the subsequent sanitisation process.'	Blancco Drive Eraser goes beyond traditional wiping methods by achieving complete sanitisation —leaving nothing behind. The process includes: • Freeze lock removal • Internal drive commands (for firmware-based erasure) • Identifying bad and remapped sectors • Hidden areas such as HPA and DCO • Drive partitions (such as MBR, GPT) • Our proprietary erasure sequence and erasure verification, which identifies malfunctions and performed processes Blancco Drive Eraser is capable of securely erasing SSDs that use ATA, SAS/SCSI or NVMe interfaces. Blancco Drive Eraser supports firmware-based erasure commands.

Learn More About Blancco Drive Eraser

The Most Certified Data Erasure Software Available

For more than 20 years, Blancco has offered solutions that help heavily regulated industries and the government comply with data protection regulations and guidelines. Our data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organisations around the world.

Now Common Criteria certified, Blancco Drive Eraser 6.9.1 provides public and private sector organisations in Australia and New Zealand a secure method of sanitising data on storage devices—regardless of underlying technology—in a cost-effective, secure and eco-friendly manner.

Increased Security Features & Support for More Drive Types

Newer BDE versions have also been developed in accordance with the minimum requirements of the Common Criteria certification. The current Blancco Drive Eraser release includes:

- Streamlined workflows that use API-enabled integrations with ERP and WMS systems to reduce human touch-time
- Support for the widest array of drive types, including Opal/TCG and SCSI/SAS self-encrypting drives, machines with Secure Boot enabled and iOS T2 devices
- Remote and simultaneous erasures across multiple drives and locations when used with Blancco Management Console
- Custom digital signatures
- Support for 802.1x authentication
- And much more

Free Trial Available

See how Blancco Drive Eraser fits within your agency environment. **Visit our website to request your free enterprise trial of Blancco Drive Eraser today**.