Blancco Earns Second Common Criteria Certification for Government Use in Australia & New Zealand

Australian agencies have additional data protection with a twice certified solution

Blancco Drive Eraser secured its second Common Criteria (CC) certification through the esteemed Australian Information Security Evaluation Program (AISEP) in June 2023. This milestone underscores the trust and assurance it provides to government data and asset managers across Australia and New Zealand. With Blancco Drive Eraser, they can confidently erase end-of-life data from a diverse range of devices, safeguarding critical information with industry-leading sanitisation software.

The AISEP is administered by the Australian Certification Authority, which resides within the Australian Cyber Security Centre. Its function is to certify products in line with rigorous international recognized security standard called the Common Criteria (aka ISO/IEC 15408), ensuring that only the most robust and dependable solutions receive certification. This second certification applies to Blancco Drive Eraser 7.3.1, verifying it meets evaluation criteria recognised by all members of the Common Criteria Recognition Arrangement (CCRA), including Australia and New Zealand. This ensures that agencies using this version can adhere to data sanitisation requirements outlined in various regulatory frameworks such as:

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

Why was Blancco Drive Eraser certified twice for Common Criteria in Australia?

Blancco follows an iterative, continuous improvement process. As we are continuously developing our software, we're also updating its certifications to ensure it continues to meet the rigorous needs of our customers. Blancco Drive Eraser's first Common Criteria Certification was granted in June 2020 for version 6.9.1. This certification remains valid for that particular version of our product until June 2025, five years from the date the certificate was issued.

Blancco Drive Eraser 7.3.1 represented a major software update that also changed the 'target of evaluation', or the specific features being tested in the software. This required that we submit the newest version for recertification to continue providing our customers in Australia with the required assurance of security and reliability. The newest certificate is valid until June 2028.

So, the result of our commitment to continuous improvement is that we now hold two valid certifications for Common Criteria in Australia and New Zealand. Our certifications can be found on the Common Criteria Portal's Certified Products List (CPL), where ACSC CC-certified products are listed and where the government's use of CPL products is affirmed.

NOTE: Products listed on the **Common Criteria Portal's Certified** Products list are considered Evaluated Products for purposes of the ISM. Inclusion in 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.

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

Common Criteria is an internationally recognised standard (ISO 15408) for evaluating information and communications technology (ICT) security products. The Common Criteria Recognition Arrangement (CCRA) 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, 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. Like its predecessor 6.9.1, Blancco Drive Eraser 7.3.1 was evaluated and certified to EAL2, which aligns with the CCRA mutual recognition.

How was Blancco's software tested for CC Compliance?

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 and 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 Blancco Drive Eraser 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 Drive Eraser v7.3.1 (PDF)**, 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** and the **NZISM**.
- 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, IEEE 2883-2022, HMG InfoSec Standard No: 5 Higher and Lower standards, BSI-GS/GSE and more.

Government agencies also benefit from Blancco Drive Eraser's scalability to create added efficiencies and optimise staff time. For instance, with it, 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 your 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, such as the Australian Government Information Security Manual (ISM), for further guidance.

Below is a sample of Australian Government ISM guidelines for media sanitisation under the sections **"Guidelines for ICT Equipment" and "Guidelines for Media"** that are fulfilled by Blancco Drive Eraser 7.3.1.

ISM GUIDELINE	HOW BLANCCO HELPS
Sanitising ICT equipment *When sanitising ICT equipment, any media within the ICT equipment should be removed or sanitised. Once any media has been removed or sanitised, ICT equipment can be considered sanitised. However, if media cannot be removed or sanitised, the ICT equipment should be destroyed as per media destruction requirements. Media typically found in ICT equipment includes:* • *electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs)* • *non-volatile magnetic memory, such as hard disks* • *non-volatile semiconductor memory, such as flash cards and solid-state drives* • *volatile memory, such as random-access memory sticks.*	Blancco Drive Eraser can detect and sanitise drives including SSDs through overwriting and, if supported, firmware erasure. It can also sanitise mSATA devices.

blancco

ISM GUIDELINE	HOW BLANCCO HELPS
Solid-state drives *"When sanitising solid-state drives, the method for sanitising non-volatile flash memory media applies."*	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 *"For non-volatile flash memory media, a technique known as wear levelling ensures that writes are distributed evenly across each memory block. This feature necessitates non-volatile flash memory media being overwritten with a random pattern twice as this helps to 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.*	Blancco Drive Eraser verifies the data sanitisation as successful and can be written to all sectors of the drive and 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 hard drives are normally not visible to a computer's Unified Extensible Firmware Interface or operating system. Therefore, any sanitisation of the readable sectors of non-volatile magnetic hard drives will leave any data contained in sectors listed in the host-protected area and device configuration overlay table untouched. Some sanitisation programs include the ability to reset non-volatile magnetic hard drives to their default state, thereby removing any host-protected areas or device configuration overlays."*	Blancco Drive Eraser goes beyond traditional wiping methods by achieving complete sanitisation —leaving nothing behind. The process includes: • Removing freeze locks • Leveraging internal drive commands (for firmware-based erasure) • Identifying and erasing bad and remapped sectors • Removing and erasing hidden areas such as HPA and DCO • Erasing drive partitions (such as MBR, GPT) • Our proprietary erasure sequence and erasure verification, which identifies malfunctions on 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.

blancco

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 14+ governing bodies and leading organizations around the world.

The newest CC certification for Blancco Drive Eraser 7.3.1 continues to provide 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 and support for more drive types

Newer Blancco Drive Eraser versions have also been developed in accordance with the 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

In just 3 minutes, see how our Common Criteria-certified Blancco Drive Eraser can save you time and reduce costs with our **Value Assessment Tool**.