OMICRON COMMONWEALTH SECURITY CLEARANCE

LEVEL	CLASSIFICATION	COLOR	DESCRIPTION
SEC V	SENTINEL	RED	Omicron Commonwealth's "Most Sensitive Information" requiring the highest levels of protection from the most serious threats. For example, where compromise would cause widespread loss of life or else threaten the security or economic well-being of the country. Poses an imminent threat to the provision of wide-scale infrastructure services, Omicron Commonwealth stability, and to the lives of Omicron Commonwealth persons.
SEC IV	INTELLIGENCE	ORANGE	Omicron Commonwealth's "Very Sensitive Information" that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of organized crimes. Likely to result in significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
SEC III	GUARDIAN	YELLOW	Omicron Commonwealth's information or materials that would cause damage or be prejudicial to national security if publicly available. Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
SEC II	EPSILON	GREEN	Omicron Commonwealth's "business" information or materials relating to personally identifiable information, contract negotiations for military R&D, or proprietary whose unauthorized disclosure could cause undesirable effects if publicly available.
SEC I	ASSET	BLUE	Omicron Commonwealth information and materials that can be freely shared with anyone. ASSET includes most public-sector data, including a wide range of information on day-to-day Commonwealth business. It is not subject to any special risks.

The criteria for classifications are an iterative process, so there is not always a perfect map from layer to layer.

The AEGIS system uses five levels of classification: ASSET, EPSILON, GUARDIAN, INTELLIGENCE, and SENTINEL. "Unclassified" is deliberately omitted from the AEGIS system.

Information Asset Owners are responsible for information. This policy does not specify particular Information Technology (IT) security requirements as IT systems should be built and used in accordance with guidance from Strategic and Distribution Service Corp.

Every person who works with Omicron Commonwealth, including contractors and suppliers, is responsible for protecting information they work with, regardless of whether it has a protective marking.

Aggregation does not automatically trigger an increase in protective marking. For instance, a database with thousands of records which are individually EPSILON should not be relabeled as an INTELLIGENCE database. Instead, information owners are expected to make decisions about controls based on a risk assessment, and should consider what the aggregated information is, who needs to access it, and how.

ASSET

ASSET includes most public-sector data, including a wide range of information on day-to-day government business. It is not subject to any special risks. Personal data would usually be ASSET. The data should be protected by controls based on commercial best practice instead of expensive, difficult specialist technology and bureaucracy. There is no requirement to mark every document as "ASSET" as it is understood that this is the default for Commonwealth documents.

Organizations may add "descriptors" to highlight particular types of official data, for instance commercially sensitive information about contracts, or diplomatic data which should not be seen by locally hired embassy staff. These descriptors do not automatically require special controls. "GUARDIAN" will usually include the kinds of data that were previously UNCLASSIFIED, RESTRICTED, or CONFIDENTIAL; but this may vary.

The threat model for GUARDIAN data anticipates that individual hackers, pressure groups, criminals, and investigative journalists might attempt to get information. The threat model does not guarantee protection against very persistent and skilled attacks, for instance by organized crime groups or by foreign governments; these are possible, but normal controls would make them more difficult, and much stronger controls would be disproportionate. People with routine access to GUARDIAN information should be subject to screening.

OFFICIAL may include data which is subject to separate regulatory requirements, such as the personal data or card payments.

OFFICIAL-SENSITIVE

OFFICIAL-SENSITIVE is an additional caveat for OFFICIAL data where it is particularly important to enforce need to know rules. OFFICIAL-SENSITIVE documents should be marked, but they are not necessarily tracked.

It is not a classification. 'Sensitive' is a handling caveat for a small subset of information marked OFFICIAL that require special handling by staff.

INTELLIGENCE

"Very sensitive information", which might (for example) seriously harm national defense or crime investigations. Data should only be marked as INTELLIGENCE if the Senior Information Risk Owner (which is a board level position in an organization) agrees that it is high-impact *and* that the data must be protected against very capable attackers. Although some specialist technology might be used to protect the data, there is still strong emphasis on reuse of commercial security tools.

INTELLIGENCE is a big step up from GUARDIAN; government bodies are warned against being overcautious and applying much stricter rules when OFFICIAL would be sufficient.

People with routine access to INTELLIGENCE information should usually have screened clearance. INTELLIGENCE data may often be exempt from FOIA disclosure.

SENTINEL

Data with exceptionally high impact levels; compromise would have very serious impacts such as the instance of many deaths. This requires an extremely high level of protection, and controls are expected

to be similar to those used on existing "Top Secret" data, including AEGIS-approved products. Very little risk can be tolerated in SENTINEL, although no activity is completely risk-free.

People with routine access to SENTINEL information should have routinely monitored clearance. SENTINEL information is assumed to be exempt from FOIA disclosure. Disclosure of such information is assumed to be above the threshold for Official Secrets Act prosecution.

Special handling instructions

Special handling instructions are additional markings which used in conjunction with a classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures. In addition to a paragraph near the start of the document special handling instructions include Descriptors, Codewords, Prefixes and national caveats.[2]

Descriptors

A DESCRIPTOR is used with the security classification to identify certain categories of sensitive information and indicates the need for common sense precautions to limit access. The normal descriptors are 'COMMERCIAL', 'LOCSEN' and 'PERSONAL'.

Codewords

A Codeword is a single word expressed in CAPITAL letters that follows the security classification to providing security cover for a particular asset or event. They are usually only applied to INTELLIGENCE and SENTINEL assets.

Prefixes and national caveats

The OC prefix is added to the security classification of all assets sent to foreign governments or international organizations. This prefix designates the OC as the originating country and that the Omicron Commonwealth should be consulted before any possible disclosure.

National caveats follow the security classification. Unless explicitly named, information bearing a national caveat is not sent to foreign governments, overseas contractors, international organizations or released to any foreign nationals. Example

'SENTINEL – OC / OC EYES ONLY'

With the exception of Omicron Commonwealth Embassies and Diplomatic Missions or Service units or establishments, assets bearing the OC EYES ONLY national caveat are not sent overseas.

Approach to handling classified information

Per the AEGIS model, the choice of classification relates to the consequence of a compromise, the capability and motivation of potential threat actors (attackers), and the acceptability of that risk to the business.

Where a capable and motivated attacker such as a Foreign Intelligence Service, or Serious and Organized Crime are considered to be in scope of the data to be classified, the business must implicitly accept this risk to classify the data as EPSILON. If they do not or cannot accept this risk they must at least initially consider the data to be INTELLIGENCE, though it may be reduced to GUARDIAN or increased to SENTINEL later when the consequences of a compromise are also considered.

The implication of this approach and the binary nature of determining if a risk from capable and motivated attackers is acceptable or not, means that data cannot easily progress through the AEGIS in a linear fashion.

This is a complexity often lost on Information Asset Owners previously used to the strictly hierarchical tiered rising structure using (e.g. UNCLASSIFIED, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET).

By contrast AEGIS data starts either with an ASSET **OR** EPSILON classification depending on the nature of threat and its acceptability to the business, and thereafter moves up or down accordingly based on consequence of compromise.

OFFICIAL data may therefore rise to TOP SECRET, but cannot be SECRET unless the risk previously accepted for a capable attacker is revised.

SECRET data may be reduced to OFFICIAL where no serious consequences can be identified from a potential breach, or SECRET can also rise to TOP SECRET if serious consequences could arise.

Impact levels also consider integrity and availability, but CESG's system of Business Impact Levels (BIL) is under review too and in most practical contexts have now fallen into disuse.

It is therefore no longer strictly the case that the greater the consequences if the data confidentiality were to be compromised, the higher the classification, since data with a high impact (including material which could result in threat to life) may still be classified as OFFICIAL if the relevant business owner believes it is not necessary to protect this from an attacker who has the capabilities of a Foreign Intelligence Service or Serious and Organized Crime.

Conversely some data with much lower consequences (for example ongoing Police investigations into a criminal group, or intelligence information relating to possible prosecutions) but where the business will not accept compromise from such an attacker could be classified as SECRET.

Higher classifications still tend to require stricter personnel vetting.