September 2020 - Round Tables

Transition to the new protective marking scheme

Questions and Answers

Below is a summary of questions posed to the Information Security Unit during the September round tables in support of organisations transition to the new protective marking scheme. The transition deadline was October 1st, 2020. Answers to each of these questions is included below. Should you wish to discuss any of this content, please email security@ovic.vic.gov.au.

Question/Comment	OVIC response
Is there a definition of 'actively using' in the context of pg. 2, bullet point 2 in VPDSF Resource: Protective-Marking-Flowchart-and-Mapping-V2.1-June-2019.pdf	'Active' essentially means information in use i.e. not archived. Organisation's should focus on assessing information that is actively used, and determine what the most appropriate protective marking is for that material. There is no expectation that organisations undertake security value assessment against information that is no longer in use or archived (i.e. inactive).
When should we update our Information Asset Register (**IAR**) to reflect the new protective marking scheme?	The IAR should be updated as part of your internal review cycle (this may differ from agency to agency). This review cycle acts a good opportunity for business units to re-evaluate the security value of their information (that they are actively using) and update the IAR with the corresponding protective marking at that time. If an information asset is no longer being actively used (i.e. has been archived), the former protective marking can remain in the IAR as it is. This former marking is referred to as a 'legacy marking' and does not have to be adjusted unless the information asset is removed from archive and is being actively used in the future. Any new entries to the IAR should reflect the new protective marking scheme.

Question/Comment	OVIC response
Who does the 1st October 2020 deadline for the implementation of protective markings apply to?	The October 2020 deadline for the implementation of protective markings is a Commonwealth deadline. For Commonwealth agencies, this is a hard deadline – organisations must transition to the new scheme by this date. Information that does not have an appropriate protective marking on it by this date may be restricted in terms of information sharing. See Information Security Manual (**ISM**) Security Control 0565 for reference. For in-scope VPS organisations, there is an expectation that protective markings will be implemented in line with this deadline. However, it is ultimately up to the organisation to manage risks associated with not meeting this deadline. There may also be other State government agencies who are taking a hard-line approach to this deadline. In light of this, organisations should consider the most appropriate way to share information. Protective markings should be applied to all types of information and medium, as appropriate, including hard and soft copy information.

Question/Comment	OVIC response
What is the relationship between protective markings and the Victorian Protective Data Security Standards (**VPDSS**)?	The VPDSS is a risk-based approach to information security. Protective markings are a security control under E2.050 of the VPDSS to mitigate risks around information handling. Protective markings denote the security value of the information and communicate a common criteria for how it should be handled (minimising the risk that it will be mishandled). The 1st October deadline for the implementation of protective markings introduces a risk that some correspondence (notably email correspondence) within government may be disrupted or delayed if it contains inappropriate, invalid or missing protective markings (see Information Security Manual (**ISM**) Security Control 0565 for reference for more information). OVIC expects that applicable entities will manage risks to public sector information in line with the VPDSS, any applicable Commonwealth Government requirements where information sharing arrangements exist, with consideration of the organisation's risk appetite, and available resources.
What if my organisation doesn't make the deadline?	Organisations that do not meet this deadline must manage the associated risks and implement any mitigation strategies when sharing information with entities operating under the new scheme post October 2020. Potential repercussions for not meeting this deadline could include disruptions or delays to correspondence with some government counterparts. For more information about the 1st October 2020 deadline (as it relates to the VPDSF), see section 3 in the information sheet in the following resource: Victorian Protective Data Security Obligations During COVID-19 V1.0.pdf

Question/Comment	OVIC response
What information should be protectively marked?	Only public sector information needing increased protection should be protectively marked. To help understand the difference between *unofficial* information and public sector information consider the following definitions: • ***Unofficial*:** Any information that has no relation to official activities, such as a personal correspondence. Unofficial information does not need to undergo the assessment process. • ***Public Sector Information*:** Any information (including personal information) obtained, generated, received or held by or for a Victorian public sector organisation for an official purpose or supporting official activities. The protective marking '**OFFICIAL'** is an optional marking that is sometimes dropped for aesthetic reasons on public release information (e.g. an annual report, website, media releases, posters, pamphlets, and letters from the public sector body Head). Notwithstanding, some email systems scan the metadata for the applied protective marking and can vet correspondence based on the marking (or lack thereof) assigned. For this reason, it may not be appropriate to exclude a protective marking from emails in some situations.

Question/Comment	OVIC response
Do Council's need to meet the deadline?	Protective markings are a security control that organisations can implement to mitigate risks around information handling. These risks will likely be present, regardless of the sector you're working in. Protective markings are an element under Standard 2 of the VPDSS. The elements provide a set of expectations around how organisations can meet the intention of a Standard. Council applicability under the VPDSS is specifically around the public entities that Council is accountable for. There is an expectation that in-scope public entities will have protective markings in place that communicates the security value of the public sector information. Additionally, if Council manages Commonwealth information, there is an expectation that this information will be protectively marked from the 1st of October 2020.
Where should the marking be held/displayed in the email - either visually and or in the email attributes?	A recent release of the VPDSF Technical Specification Email Protective Markings provides examples of how to display these markings in emails. In section 14 of the Email Protective Marking Standard (Version 2018.4) there is reference to the position of the marking in the subject field and caution offered in footnote 4 of the same document. Table 21 of the same document also provides examples of protective markings using Internet Message Header Extension Markings, and depicts how these protective markings can be presented visually as well.

Question/Comment	OVIC response
Will there be a conflict across the different Marking tools that are being used - O365, Janus and Titus, in terms of detecting the marking at the email gateway?	It all comes down to the implementation of the particular email marking tool. The Email Protective Marking Standard (version 2018.4 being the most current release) sets out technical specifications for the implementation on emails, regardless of the tool. OVIC has also recently released the VPDSF Technical Specification Email Protective Markings which outlines specific implementation guidance for Vic Gov organisations.
When you talk about 'applying' the markings, are you talking about tools outside of the Electronic Document and Records Management System (**EDRMS**) for doing this? What tools are these?	There are a variety of tools that can help users apply protective markings to emails and documents, however OVIC cannot recommend a particular solution or vendor. Instead, we suggest you search for 'protective marking solutions' and consider the most appropriate solution for your organisation (for example Janus, Titus, Preemptive, Microsoft Azure Information Protection (**AIP**)).
Councils have proactive role to share and receive information or advising stakeholders. If one organisation doesn't use email protective markings, will this cause issues?	Organisations who don't implement the new scheme by October 1st, 2020 may experience some issues. Some of these issues could include emails being rejected by other government bodies who have implemented particular rules to block incoming correspondence (i.e. Information Security Manual Control 0565 states' *Email servers are configured to block, log and report emails with inappropriate protective markings*'). Organisations should also consider the risk of users or recipients of the information not necessarily understanding the confidentiality requirements of the material if it does not have a protective marking applied to it.
When must all organisation have protective marking implemented by?	The deadline for transition to the new protective marking scheme is October 1st, 2020

Question/Comment	OVIC response
Does information that is public (e.g. a presentation) need to have a marking?	For information that has been approved for release to the public (following the authorisation and governance arrangements of your organisation), it is not compulsory to label this material with an OFFICIAL marker. This could include presentations that have been authorised for public release, or letters or brochures that have been designed with public release in mind.
If an email has a marking, does this apply to the attachments in an email?	Control 0270 of the Information Security Manual states '*Protective markings are applied to emails and reflect the information in their subject, body and attachments*'. This means that the protective marking applied to the email needs to reflect the highest security value of the combined content of the email (i.e. body of the email), as well as any attachments. It does not mean that the protective marking applied to the email is, by default, the same marking of any / all of the attachments. Instead it means that the combined, overall value of the contents and attachments = *X Protective Marking.* It is worth noting, that it is the responsibility of the originator to perform a security value assessment of the content of these attachments, ensuring an appropriate protective marking is applied to this material (N.B. the originator of the attachments may be different to the originator of the email). This process is particularly important as attachments can be downloaded and used separately. If the attachments are used independently of the email, the protective marking applied to the individual documents act as a visual signal of the confidentiality requirements of that particular material.
Our current landscape for information is changing considerably and so we must update our policies to reflect this. Any there any new resources like information security policies?	OVIC will continue to publish resources under the VPDSF Resources page, but there are no current releases planned around information security policies. OVIC will look to publish a high-level version of our own internal security policy, pending internal approval. Please note - this would act as a sample only, and your own organisational circumstances must be taken into account when framing your own information security policy.

Further Information

Contact Us

t: 1300 00 6842
e: security@ovic.vic.gov.au
w: ovic.vic.gov.au