Checklist for Rule 5: Security of biometric information

In general, you need to consider:

- ✓ How will you **protect** the biometric information within your system? Protecting information means protecting it from loss and unauthorised modifications. Protecting information includes technical controls (e.g. encryption), physical controls (e.g. locked rooms) and organisational controls (e.g. policies governing how biometric information is stored – such as storing biometric information locally if appropriate).

- ✓ How will you ensure **devices and software** are kept up to date by applying the latest updates and patches?

- ✓ Where and how is information stored? Will the biometric information be **kept separate from** (e.g. not linked or connected to) **other information** in your system? If it is necessary to link it to other information, what other protections can be put in place? Do you need to store the information on a central system, or can you store it across local devices i.e. on-device verification?

- ✓ What is your plan for information **backups**?

- ✓ How will you **restrict access** to biometric information? How will you ensure only authorised people have access? (e.g. individual user logins and regular and random audits). Who is responsible for controlling access? How will you limit and identify employee browsing?

- ✓ How will you **restrict the use and disclosure** of biometric information? Can you build in technical restrictions as well as having organisational policies about the use and disclosure? Who is responsible for making these decisions?

- ✓ How will you assess whether your **safeguards are operating effectively**? What is your **vulnerability management** process?

- ✓ How are you **minimising data collected, stored and retained**? The less information you hold, the less information you have to protect. If you do not need to retain biometric information, you should delete it – for example, if you only need to retain biometric templates and not samples, you should delete the biometric samples as soon as they are processed into templates.

- ✓ How will you **safely dispose** of biometric information when it is no longer needed for your lawful purpose? Are your disposal methods appropriate for the type of information concerned? When will you dispose of biometric information?

- ✓ What **staff training** will be in place for staff involved in your biometric system?

- ✓ What is your organisation's **capability** in this area? While the size and resources of your organisation is a factor in what is reasonable, you must still ensure you have enough capability to securely deploy and manage a biometric system. This is an important consideration as off-the-shelf biometric systems become more widely available.

- ✓ If you are using a **third-party provider** to hold biometric information on your behalf, what are your rights and ability to monitor and audit that provider's security practices? What are your residual responsibilities? See our guidance on working with third parties for more information. Remember that if the third-party provider is holding the information on your behalf and not using the information for their own purposes, you are still responsible under the Privacy Act.

- ✓ What is your plan for if **something goes wrong**? Security breaches can lead to privacy breaches, but even a security breach that does not directly cause a privacy breach could weaken the biometric system and needs to be promptly addressed. Remember that if you have a privacy breach that either

has caused or is likely to cause anyone serious harm, you must notify the Privacy Commissioner and any affected people as soon as you are practically able. See our privacy breach guidance for more information.

- ✓ Does the biometric data involve content **sensitive for Māori** e.g. moko kanohi or moko kauae and how will you address it? What mitigations are available to you to avoid breaches relevant tikanga? Have you consulted experts if appropriate?

- ✓ Can you meet **technical guidance** from relevant international bodies or experts? E.g. can you meet relevant ISO/IEC standards for protecting biometric information?