**Authentication Factor Level Table - template**

This template provides a framework for documenting how Authentication Assurance controls with different levels are being met.

A separate template should be completed for each access channel and different Authenticator implemented.

If an authentication factor is not part of the Authenticator being implemented, the relevant table can be deleted.

If a control for an authentication factor does not apply for the level being sought, enter NA.

***Channel and target authentication level***

General information about the Authenticator being used

|  |  |
| --- | --- |
| **Authentication channel** | This Authenticator is to be used access *<describe if it is a system, location, or other function>.*  Presentation of the Authenticator is *<describe if it is in-person, over the phone, via the internet, or some other mode>***.** |
| **Authenticator description** | *<Describe the type of Authenticator being established, including which factor/s it uses.>* |
| **Level of Authentication Assurance (LoAA)** | The level of authentication assurance (LoAA) being achieved is **Level *<number between 1 and 4>.*** |

***All authentication factors***

The following controls are not specific to any authentication factor. *Enter NA if they do not apply to the level stated above.*

|  |  |  |
| --- | --- | --- |
| **Control** | **Control description** | **Process** – Describe how the control is being met for the level, enter NA if not applicable for the level. |
| **AA2.03** | The RP limits the ability to share an authenticator by implementing 2 different factor types. |  |
| **AA2.04** | The RP allows no more than 30 consecutive unsuccessful attempts to authenticate by any factor, disables the account and triggers further investigation. |  |
| **AA4.02** | The RP establishes if the Authenticator has been previously compromised to the extent it makes it unusable. |  |

***Knowledge factors***

The following controls are specific to knowledge factors. *Delete this section if knowledge factors are not used as part of the Authenticator.*

|  |  |  |
| --- | --- | --- |
| **AA7.01** | The RP implements minimum levels of complexity on any knowledge factor response (secret). |  |
| **AA7.02** | The RP limits the creation of easily guessable knowledge factor responses by disallowing repetition or patterns and where the authenticator has the form of an online password, apply the following exclusions (as applicable to the character sets being used):  • disallow repetitive or sequential characters  • disallow specific words, for example the identifier (e.g. username), name of the service etc.  • disallow singular dictionary words and common character substitutions  • disallow passwords contained in blacklists (usually include overly common combinations and compromised passwords) |  |
| **AA7.03** | The RP implements maximum limits for unsuccessful attempts and prevents further attempts for a minimum period. |  |
| **AA7.04** | The RP prevents use of a guessed or discovered knowledge factor by combining it with an authentication factor of another type. |  |

***Possession factors***

The following controls are specific to possession factors. *Delete this section if possession factors are not used as part of the Authenticator.*

|  |  |  |
| --- | --- | --- |
| **AA8.01** | The RP prevents use of a physically acquired possession factor by combining it with an authentication factor of another type. |  |
| **AA9.02** | The RP uses dynamic, non-predictable responses to non-physical challenges on possession factors and limits the response validity to a maximum of 10 minutes or 1 minute, where little messaging delay exists. |  |
| **AA9.03** | The RP MUST, for responses to non-physical challenges on possession factors, utilise a minimum complexity of:  • 6 numeric characters; or  • 4 alphanumeric characters; or  • an equivalent level for other codes such as pictograms. |  |

***Biometric factors***

The following controls are specific to biometric factors. *Delete this section if biometric factors are not used as part of the Authenticator.*

|  |  |  |
| --- | --- | --- |
| **AA9.04** | The RP addresses spoofing of biometric challenges by ensuring the biometric response is obtained from the person using appropriate measures to detect spoofing attempts (e.g. recordings, masks, makeup or prosthetics etc.). |  |
| **AA9.05** | The RP obtains biometric factor samples in person or remotely incorporating liveness checking which demonstrates at least 90% resistance to presentation attacks. |  |
| **AA10.01** | The RP reduces the occurrence of false positives in biometric comparisons by using:  • manual comparison of the biometric characteristic by a trained operator  • systematic comparison with a rate of <0.01% false positives, based on a one-to-one comparison. |  |
| **AA10.02** | The RP protects against the probabilistic nature of biometric comparisons by combining it with an authentication factor of another type. |  |