**Enterprise Information Security Policy Exception Request Instructions**

This process and accompanying form are used to formally request an exception to the Commonwealth’s Enterprise Security Policies and Standards.

Please read these instructions prior to completing the Exception Request form. If you have any questions regarding the Exception Request Process, or the form, contact EOTSS-CentralizedIntake@mass.gov.

* Download the form by clicking the link at the end of these instructions. Note: The form must be submitted in Microsoft Word format (i.e. .docx); other formats, including PDF, will not be accepted.
* Fill in the form as completely as possible, including all requested information about the system and business requirement for the requested exception. Required information includes but is not limited to:
	+ Enterprise Policy/Standard: (i.e. IS.003 - Access Management Standard) and the specific Standard Statement: (i.e. 6.4.1.1: password length at least 12 characters) for which an exception is being requested
	+ The specific device, application, and/or service for which the exception is being requested, along with its criticality (i.e. High, Medium, Low)
	+ Data classification (i.e. HIPAA, PII, FTI etc.) of associated device, application, and/or service
	+ The nature of the non-compliance (i.e. application does not allow 12 character passwords)
	+ Explanation for why exception is being requested, what business need or situation exists, what alternatives were considered, and why they are not appropriate
	+ Analysis of the potential risk posed by non-compliance (if the exception is granted) (i.e. smaller passwords are easier to crack, creating a higher risk of compromise)
	+ Plan for managing or mitigating those risks (i.e. compensating controls, alternative approaches)
	+ Anticipated length of the requested exception (typically 30-90 days) Note: Permanent Exceptions will **not** be granted, per EOTSS CISO
* Manager/Supervisor approval is required and must be obtained via email.
* System/Data Owner (C-Level) approval is required and must be obtained via email – Note: Requests cannot be considered without these documented approvals.
* Submit request by navigating to the EOTSS Service Catalog in ServiceNow.
	+ In the Service Catalog click “Security and Firewall”
	+ On the Security and Firewall page click “Security Policy Exception”
	+ Attach completed form and all approval emails to request in ServiceNow – Click “Order Now”.

The EOTSS Governance, Risk, and Compliance (GRC) Team will make every attempt to process exception requests as quickly as possible. In most cases GRC would expect to complete the review process in about 7 business days.