**Department Admin Selection API**

**Description:** An API creation for Department admins as students or learner can select the trainers based on the requirements. Main admin have the accessibility to create, update and delete the data’s.

**Last Update Status:** updated December, 2020

# Overview

Course Admin API consist of 4 API for getting, posting, updating and deleting. Schema are used in model folder so that the data is filtered every time when it is posted by any user. It designed in such a way that if other developer faced any error’s they can sort the error easily, also get detail view by seeing the console itself. Along with the API we also gone through pagination and partial response.

# Purpose

The purpose of this policy is to establish a standard for creation of API’s and the protection and handling of API’s.

# Scope

The scope of this policy includes all the API who have the responsible to create a service. Implementation of caching, error handling, pagination and partial Response. As user feel easy and use full while going through this.

# Policy

4.1 Pagination

If the data is more after the deployment or in production user fell disturb to see and search. Where pagination limiting the count of retrievals from database.

Example: You have to read 100 documents, instead of read whole in a single try reading part by part. That is pagination

4.2 Partial Response

Is nothing but a getting response from data as per the user or developer requested. Suppose we have 10 fields in 1 document where we can select the fields we required.

4.3 Caching

Caching is a technique of storing frequently used data or information in a local memory, for a certain time period. So, next time, when the client requests the same information, instead of retrieving the information from the database, it will give the information from the local memory

4.4 Error Handling

Take advantage of language specific semantics and represent when something exceptional has happened. Exceptions are thrown and caught so the code can recover and handle the situation and not enter an error state. Exception can be thrown and caught so the application can recover or continue gracefully

# Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

# 5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

# Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

Password Construction Guidelines

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| November 2020 | SANS Policy Team | Updated and converted to new format. |
| December, 2020 | SANS Policy Team | Updated to confirm with new NIST SP800-63.3 standards. |