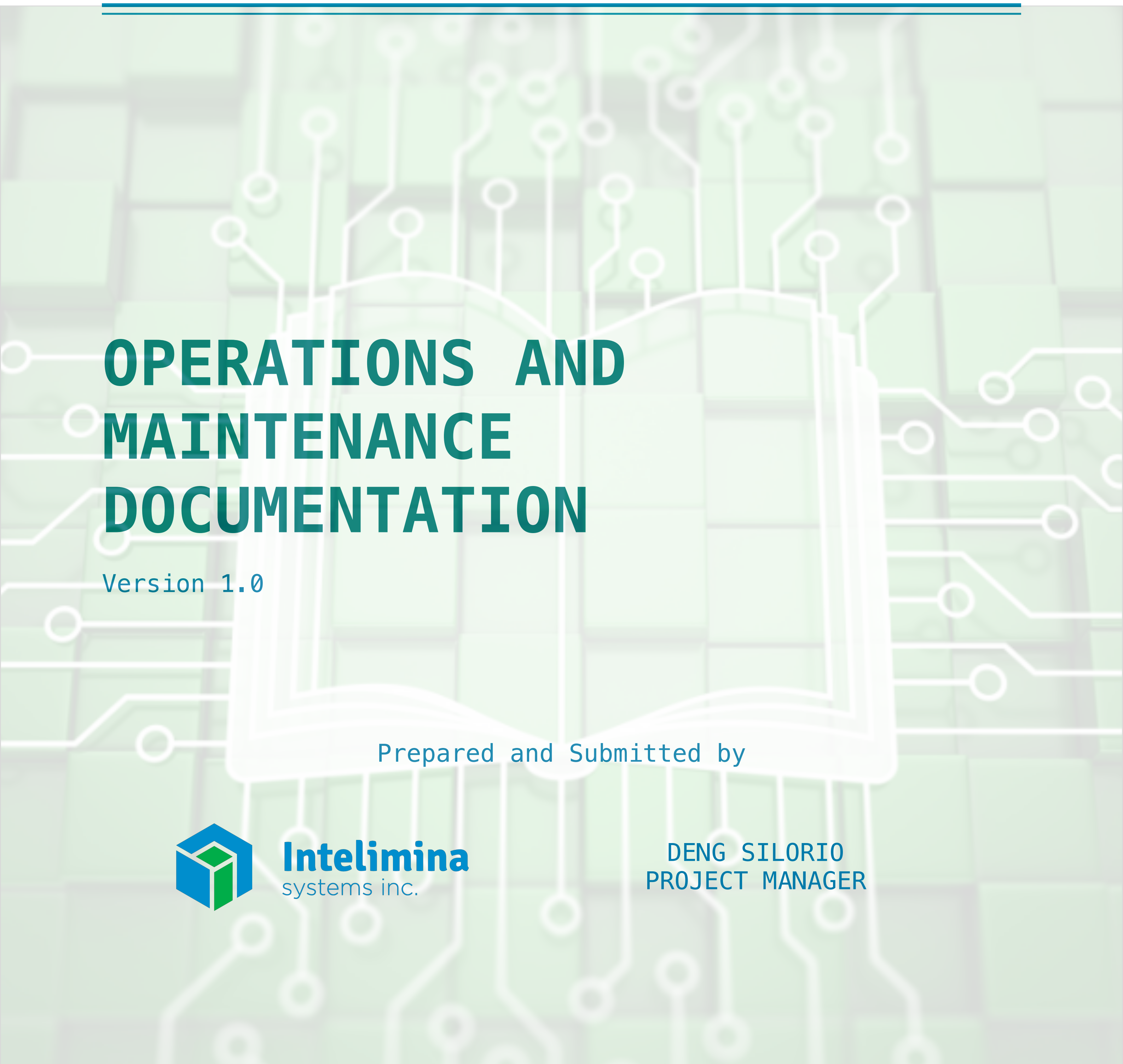
Procurement of the Supply, Delivery of One-Year Subscription for

DepEd Commons for Unlimited Users with Support Services

CONTRACT# 2020c-BLR4(005)-BII-CB009-C028



OPERATIONS AND MAINTENANCE DOCUMENTATION

Version 1.0

Prepared and Submitted by

Intelimina
systems inc.

DENG SILORIO
PROJECT MANAGER

Content

Table of Figures

Appendices

Appendix A: Web Application Security Policy

Appendix B: Server Security Policy

Appendix C: Database Credentials Coding Policy

Appendix D: Remote Access Policy

Change History

Version	Date	Author	Section	Summary
1.0	06/21/2021	Intelimina		Initial draft

Abbreviations

CI	Curriculum and Instruction
CO	Central Office
DITO	Division IT Officer
FAQ	Frequently Asked Question
IdP	Identity Provider
IUSC	Intelimina User Support Center
LRP	Learning Resource Portal
O&M / OM	Operations and Maintenance
OER	Open Educational Resources
PBDs	Philippine Bidding Documents
QA	Quality Assurance
SLA	Service Level Agreement
SSO	Single Sign On
SysAd	System Administrator / System Administration
TOR	Terms of Reference
UAT	User Acceptance Test

1. Introduction

The DepEd Commons, powered by Grado Network and implementing Grado Learning Resource Portal (LRP) Module, is a turnkey service that allows DepEd stakeholders — administrators, staff, instructors, and learners — to be driven and inspired in using a dynamic yet simple tool for managing DepEd's learning resources and OERs. Grado LRP's primary goal is to drive down the cost and to drive up the quality of an institution's files and documents repository by streamlining its authentication, monitoring, evaluation, approval, and archival policies.

For the teachers, it will serve as a tool to improve and imbibe their competencies. For the students, it is envisioned as a catalyst to transform and adopt digital learning guided by a community.

As Secretary Liling Briones stated, "Education must continue even in times of crisis whether it may be a calamity, disaster, emergency, quarantine, or even war."[1]

1.1. General Objectives

1.1.1. To plan, provision, and implement MS Azure infrastructure appropriate for DepEd commons;

1.1.2. To install, configure, and implement the necessary DepEd Commons modules;

1.1.3. To serve both the public and private school teachers and learners;

1.1.4. To ensure that the deployment of the DepEd Commons platform is secure, reliable, and scalable.

1.2. Document Description

This Operations and Maintenance Document describes the general administration, management, and support of the DepEd Commons that is procured under CONTRACT NO. 2020c-BLR4(005)-BII-CB009-C028. This

[1] https://www.deped.gov.ph/2020/03/21/learning-while-staying-at-home-teachers-parents-support-deped-distance-learning-platform/

Document works in conjunction to these artifacts:

1.2.1. Technical Specifications and General Requirements/ Specifications[2]

1.2.2. Testing Parameters[3]

1.2.3. System Design Document[4]

1.2.4. User Guides[5] for the following Users

1.2.4.1. Students

1.2.4.2. Teachers

1.2.4.3. Uploaders

1.2.4.4. Publishers

1.2.4.5. Approvers

1.2.4.6. CI Approvers

1.2.4.7. Division IT Officers

1.2.4.8. Central Office Staffs

1.2.4.9. Super Administrators or Superadmin

This Document may lift and summarize contents from the artifacts mentioned above. The user guides, on the other hand, shall be kept and maintained by Intelimina until the end of the SLA period. They shall be the basis, too, of the Intelimina User Support Center (IUSC)'s basic help scripts and FAQs.

[2] Section VII of PBDs 2020c-BLR4(005)-BII-CB-009 also titled "Supply and Delivery of One-Year Subscription for DepEd Commons for Unlimited Users with Support Services," pp. 38-44. This also includes appended SLA taken from Bid Bulletin No. 1 dated November 2, 2020.

[3] Annex D of PBDs 2020c-BLR4(005)-BII-CB-009

[4] This is submitted together with this document.

[5] The link to the online user guides is https://bit.ly/3zjey3N. Documents are on view and download permissions. Revisions are done depending on updates made to the application.

2. Operations & Maintenance Structure

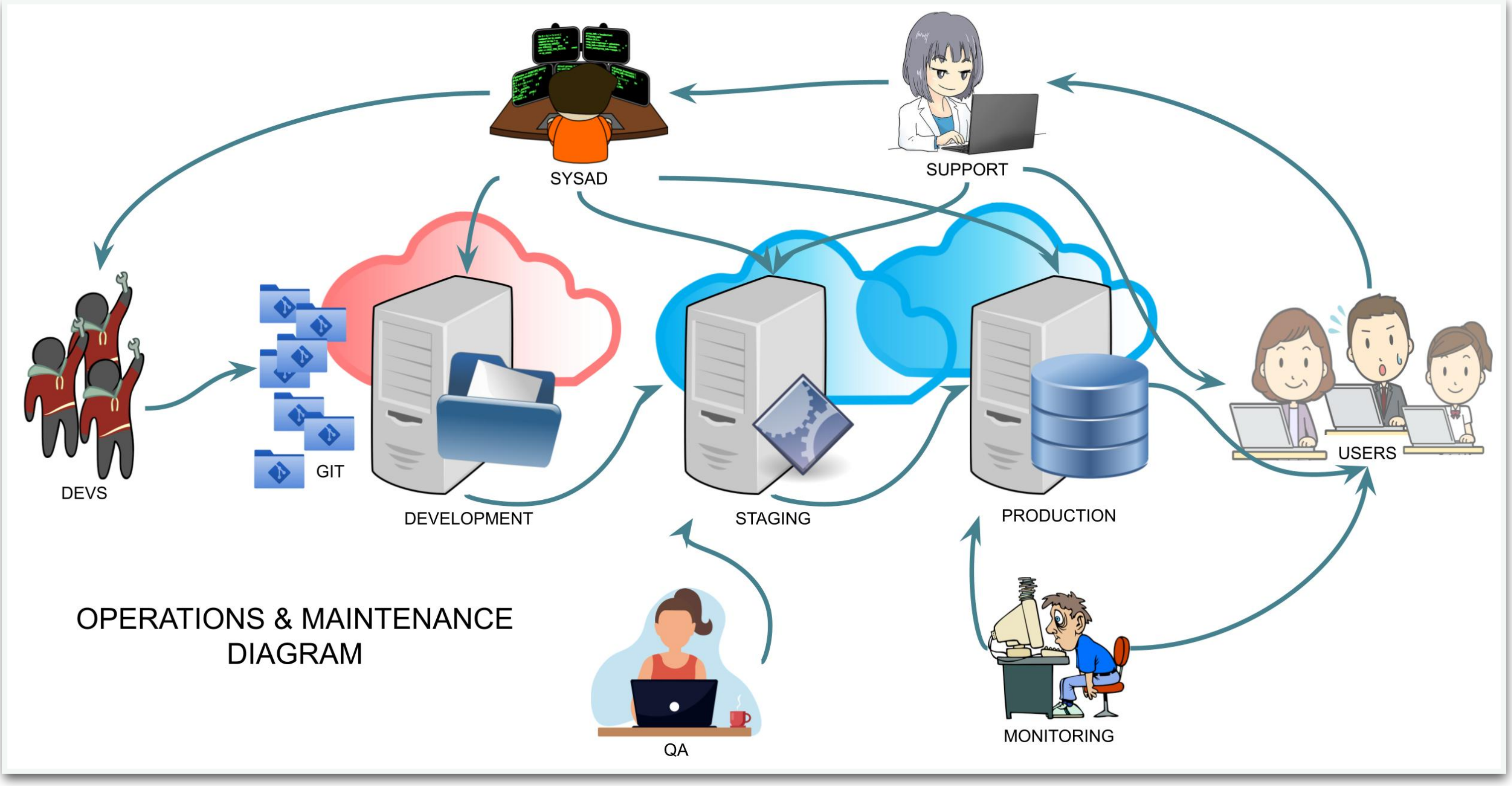


Fig. 1. Overview of Roles and Components Interaction in the O&M Environment

2.1. Processes

2.1.1. Development

Code development, modification, enhancement, bug fixes, and deployment are performed during Development. Developers may set up their own development environ but should use git for code version control.

2.1.2. Staging

Also called the Testing stage, the Staging phase involves strict Quality Assurance prior to code deployment in the Production or live site. Only when Development has passed the QA stage can the codes and fixes see Production.

2.1.3. Production

Web and mobile applications in Production are what actual and live Users access. Issues or problems encountered by Users are reported to Support. Support Team then checks and replicates issues as reported. Support either provides resolution or submits errors to the System Administration Team which in turn further checks the error, resolves it, or courses the same to the Development Team if needs fixes.

2.1.4. System Administration

System Administration involves ensuring smooth operations of the whole system and that all its components are working smoothly. This is a tedious task that involves both manual and automated checks and supervision.

2.1.5. Monitoring

The Monitoring Team's task is almost identical to System Administration's in that it entails ensuring that Production is at its best performance at all times. This also means that it is the team that ensures that User satisfaction is maintained at the highest level every single day.

2.2. Server Details

The Production Environment is shown in detail in *Fig. 2*. Its server and software components are described in the succeeding tables.

Server Name	IP Address	Specifications
DEPEDCOMMONSPROD	52.230.6.183	8 vCPU, 64GB RAM
DEPEDCOMMONSPROD2	20.44.218.250	4 vCPU, 16GB RAM
DEPEDCOMMONSPROD3	13.67.69.52	4 vCPU, 16GB RAM
DEPEDCOMMONSPROD4	13.67.58.243	2 vCPU, 16GB RAM
DEPEDCOMMONSPROD5	15.148.89.231	4 vCPU, 16GB RAM
DEPEDCOMMONSPROD6	20.191.143.143	4 vCPU, 32GB RAM
DEPEDCOMMONSPROD7	13.76.218.40	4 vCPU, 32GB RAM

Database	IP Address	Specifications
PostgreSQL	DEPEDCOMMONSPROD	8 vCPU, 64GB Storage

Cache Server	IP Address	Specifications
REDIS	DEPEDCOMMONSPROD	8 vCPU, 64GB Storage

Application Gateway	IP Address	Specifications
CDN	20.197.66.172	1 instance of WAF v2, autoscaling to 6 instances

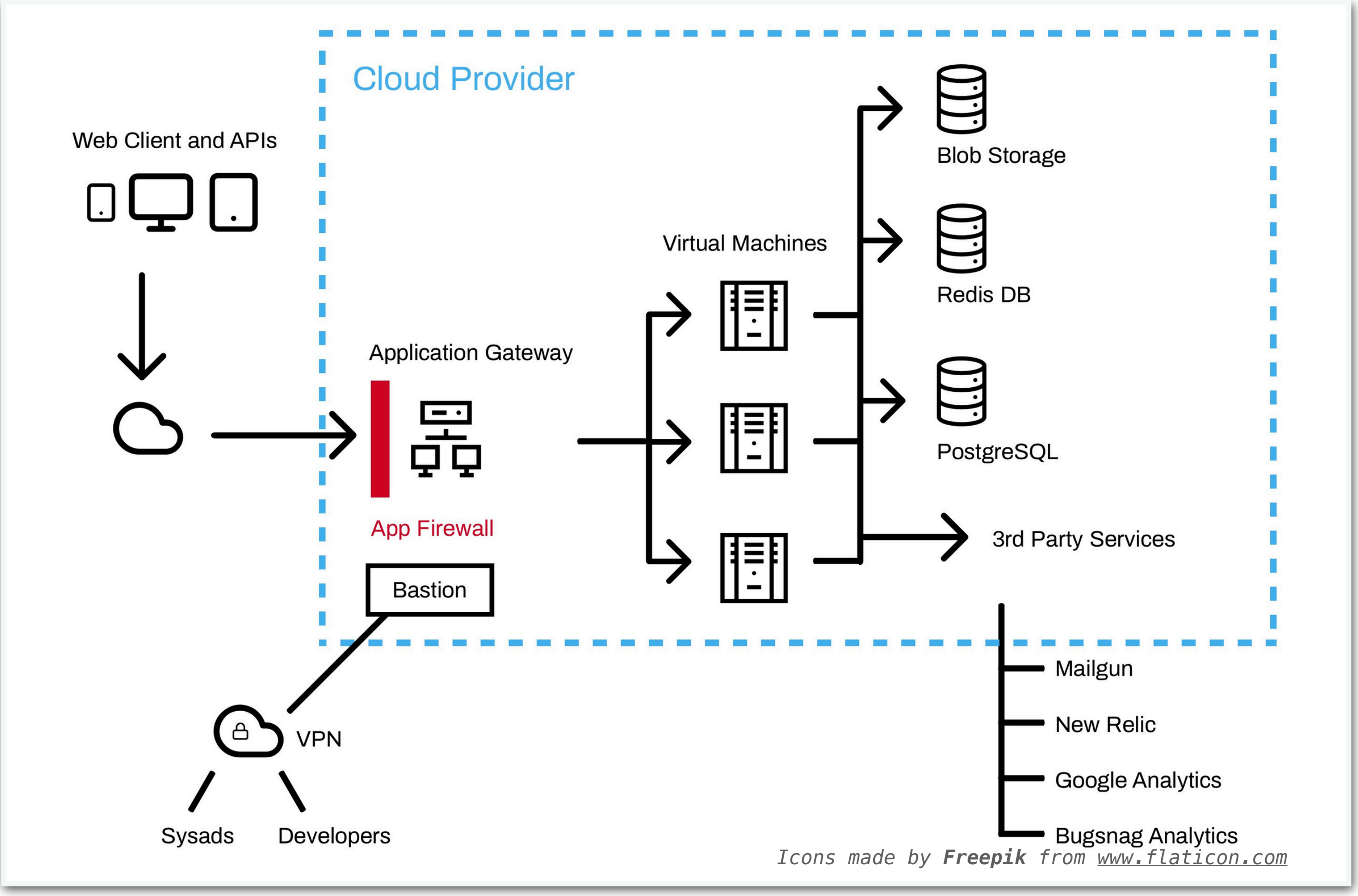
3. Software Components

3.1. Language

3.1.1. Ruby 2.7.2 (https://www.ruby-lang.org/en/)
Ruby is a dynamic, open source programming language with a focus on simplicity and productivity.

3.1.2. Python 3.0 (https://www.python.org)
Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together.

3.1.3. Javascript (https://developer.mozilla.org/en-US/docs/Web/JavaScript)
JavaScript or JS is a lightweight, interpreted, object-oriented language with first-class functions, and is best known as the scripting language for web pages, but it's used in many non-browser environments as well. It is a prototype-based, multi-paradigm scripting language that is dynamic, and supports object-oriented, imperative, and functional programming styles.



Icons made by ***Freepik*** *from* *www.flaticon.com*

Fig. 2. Production Environment Application and Network Diagram

3.2. Framework

3.2.1. Ruby on Rails 6.0 (https://rubyonrails.org)
Ruby on Rails is an open-source web framework that's optimized for programmer happiness and sustainable productivity. It lets you write beautiful code by favoring convention over configuration. DepEd Commons is written on Ruby on Rails which uses Ruby as its programming language.

"Rails", "Ruby on Rails", and the Rails logo are registered trademarks of David Heinemeier Hansson.

3.2.2. ReactJS 16.13.1 (https://reactjs.org/)
ReactJS is a library of JavaScript programming languages. It is used to build a high-intensity user communication for web applications.

3.2.3. Active Admin 2.7.0 (https://activeadmin.info/)

Active Admin is a framework for creating administration style interfaces. It abstracts common business application patterns to make it simple for developers to implement beautiful and elegant interfaces with very little effort.

3.3. Database

3.3.1. PostgreSQL 10.15 (https://www.postgresql.org)
PostgreSQL is a powerful, open source object-relational database system that uses and extends the SQL language combined with many features that safely store and scale the most complicated data workloads. The origins of PostgreSQL date back to 1986 as part of the POSTGRES project at the University of California at Berkeley and has more than 30 years of active development on the core platform.

3.3.2. Redis 4.0.9 (https://redis.io)
Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. Redis provides data structures such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperloglogs, geospatial indexes, and streams.

3.4. Web and Application Servers

3.4.1. nginx 1.16.1 (https://nginx.org/en/)
nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server, originally written by Igor Sysoev. It is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption. For DepEd Commons, nginx will be used to serve up static assets and to reverse proxy requests to the different application servers, based on URL.

3.4.2. Puma 3.12.6 (https://puma.io)
Puma, built for speed and parallelism, is a small library that provides a very fast and concurrent HTTP 1.1 server for Ruby web applications.

3.4.3. Sidekiq 6.0.7 (https://sidekiq.org)
Sidekiq is a full-featured background processing framework for Ruby. It aims to be simple to integrate with any modern Rails application and much higher performance than other existing solutions.

3.5. Third-party Services

3.5.1. Azure Storage (https://azure.microsoft.com/en-us/product-categories/storage)
Microsoft's cloud storage provides highly scalable, secure, performant, and cost-effective foundation to run business applications.

3.5.2. Amazon S3 (https://aws.amazon.com/s3)
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

3.5.3. Git (https://git-scm.com)
Git is a free and open source distributed version control system designed to handle everything from small to very large projects with speed and efficiency.

3.5.4. Mailgun (https://www.mailgun.com)
Mailgun is an all-in-one intelligent email delivery platform.

3.5.5. New Relic (https://newrelic.com)
New Relic is a web application service designed to monitor server performance and availability.

3.5.6. Bugsnag (https://www.bugsnag.com)
Bugsnag is an error monitoring and reporting software.

4. System Overview

4.1. System Users

There are five (5) main DepEd Commons users: admin, student, teacher, uploader, and approver. There are also nested users. These are users that have the same access but different permissions from a main user — DITO admin, CO admin, CI Approver admin, Publisher (quasi-Approver), and non-teaching DepEd users (nested as a user type under Teachers). To date, the estimated number of users that accessed the DepEd Commons are shown in Table 1.

Users	Est. number as of June 21, 4PM
Superadmins	10
DITO admins	224
Central Office admins	2
CI Approver admins	3
Uploaders	30
Publishers Only	3
Approvers/Publishers	15
Unknown Guests (until recently, no status was required to access DepEd Commons)	73,471,729
Students (Guest)	5,088,196 out of 80,595,204
Students (Registered/Confirmed)	100,408 out of 18,307,672 migrated accounts
Teachers (Guest)	2,035,279 out of 80,595,204 migrated accounts
Teachers[6] (Registered)	484,579 out of 1,054,976 migrated accounts

Table 1: Estimated number of DepEd Commons system users

4.2. Functional System Overview

4.2.1. System Users Access and Control

OERs is DepEd Commons' pulse. In Grado LRP, all users have specific permissions granted them. *Fig. 3* shows the current

[6] Non-teaching DepEd personnels are nested under this group. Users, on profile update, are required to choose whether they are currently teaching or non-teaching staffs. Statistics of teaching vs non-teaching personnel can be extracted as a report.

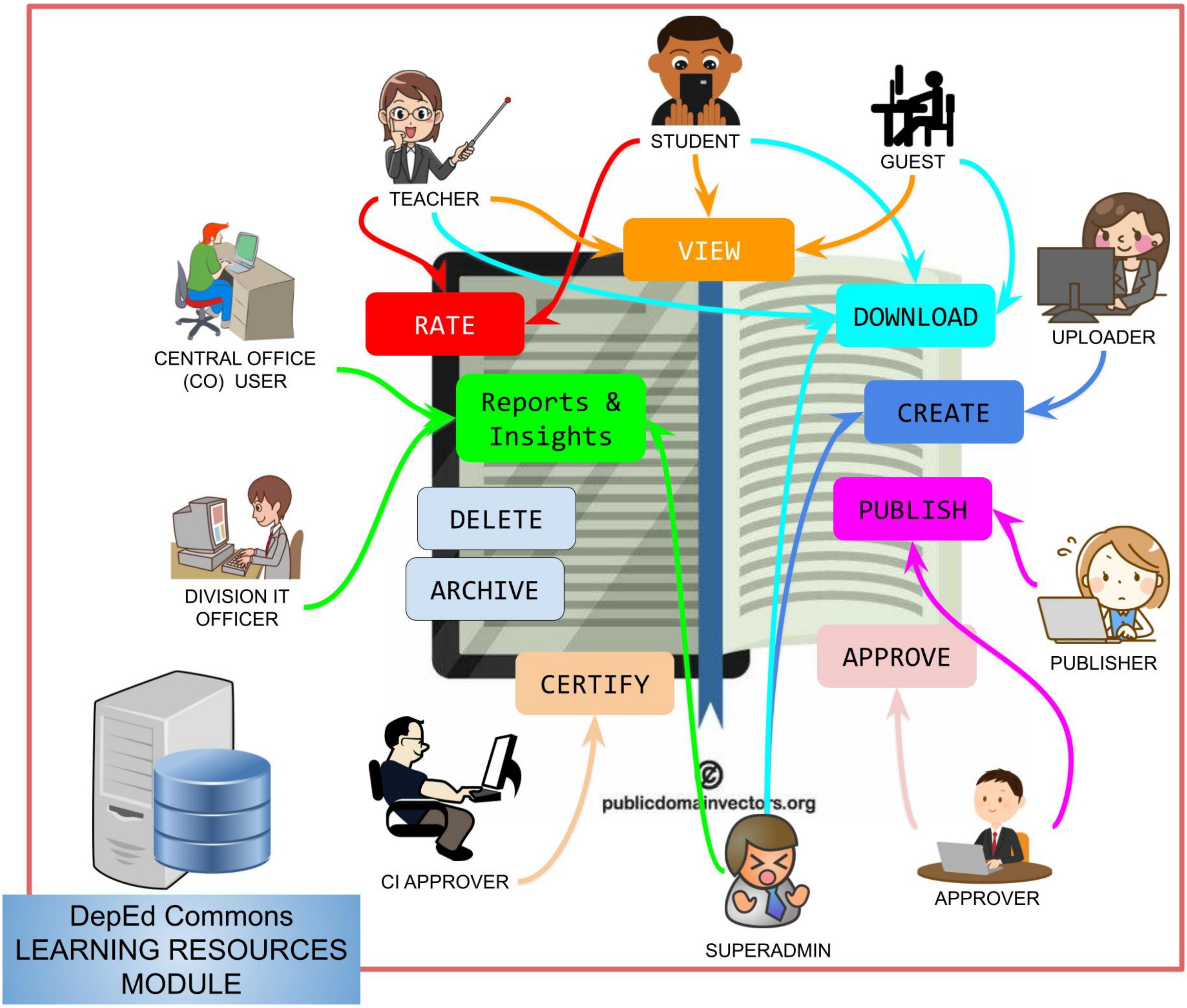


Fig. 3. DepEd Commons System Users Access and Control Diagram

Access Control for all system users.[7]

4.2.2. Learning Resource Attributes

The TOR required a number of learning resource attributes. *Fig. 4* shows how these are implemented in the DepEd Commons, what these attributes are, and which users can access them.[8]

[7] Specific tasks and functions of each user is presented in the *User Guides*.

[8] A detailed explanation of each attribute and how this is managed in the DepEd Commons, the attributes are specified in the *System Design Document*.

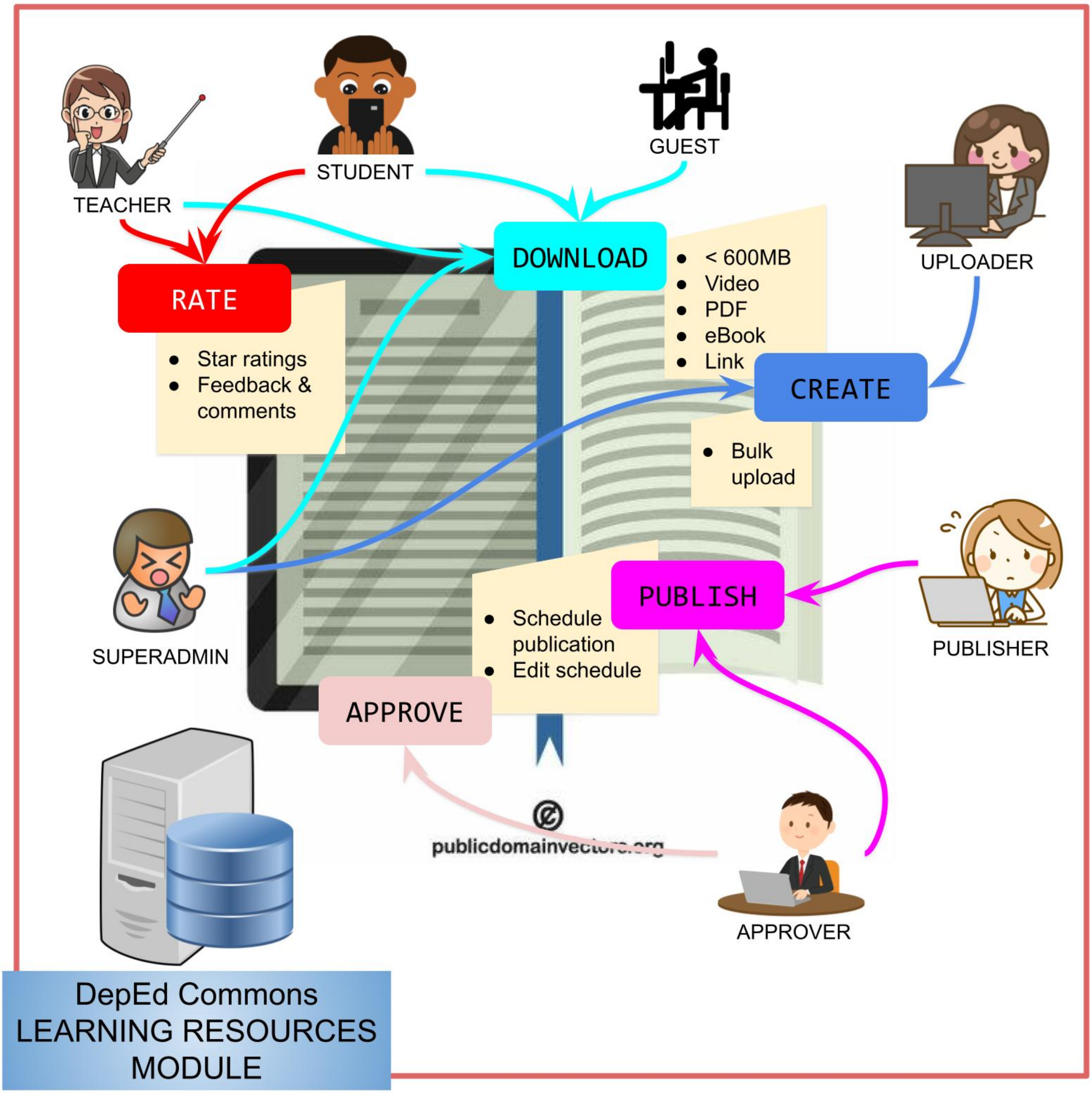


Fig. 4. TOR-based Learning Resource Attributes by User Access

4.2.3. Learning Resource Definitions

The TOR also required that learning resources have proper denotations.[9] Being the central character that brings life to the entire system, learning resources are generally qualified and quantified in every aspect. Its minimum characteristics and definitions are shown in *Fig. 5*.

[9] A detailed administration procedure for each is specified in the *System Design Document.*

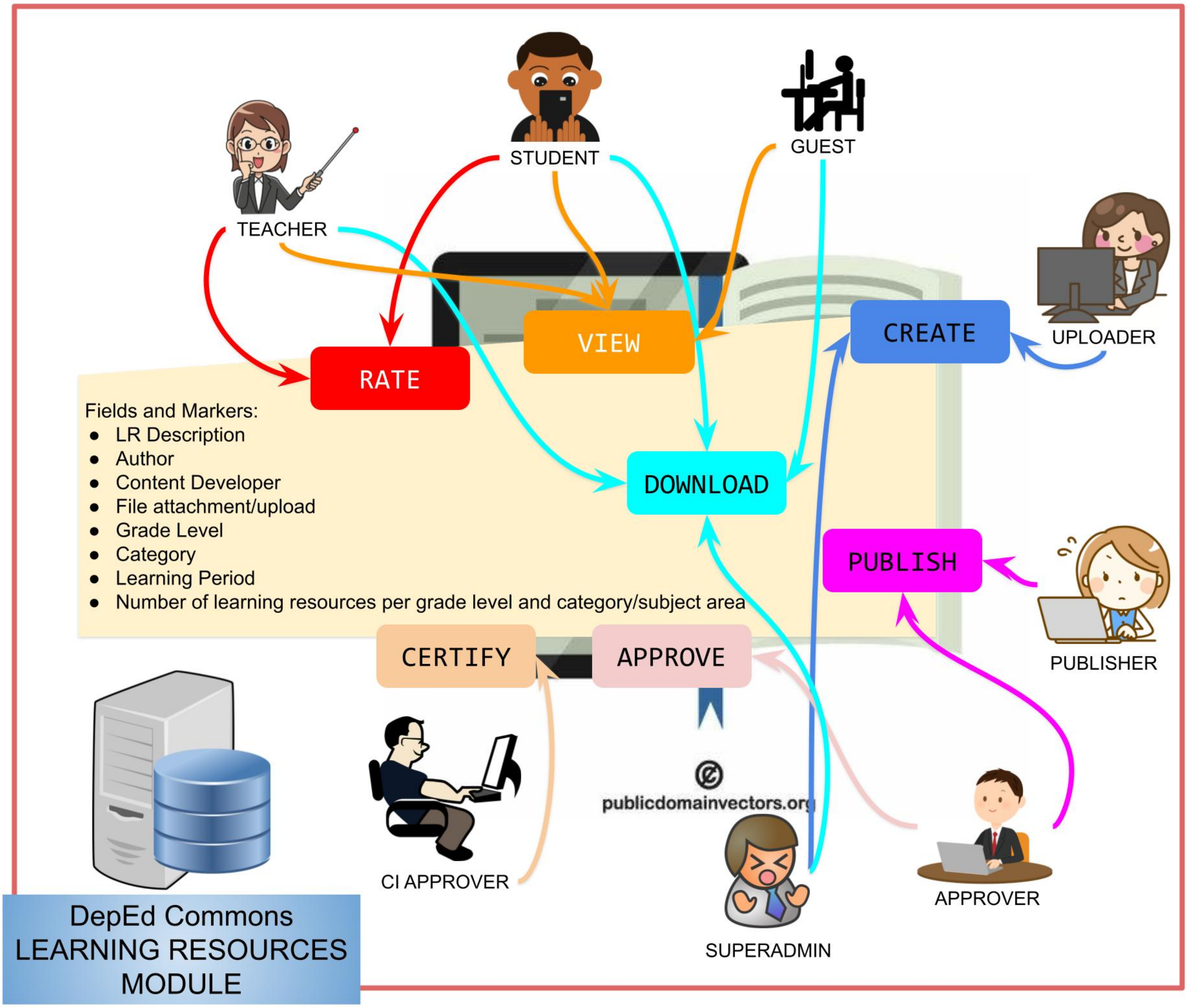


Fig. 5. Learning Resource Minimum Denotations

4.3. Peak Processing Time[10]

Busiest Days: Monday-Wednesday

Busiest Times: 8:00 - 11:00AM, 1:00-2:00PM

4.4. Processing Overview

The following policies are currently enforced governing the use of DepEd Commons.

[10] The information and figures were based on Google Analytics Insights for “Users per time of day” from January 1 - June 21, 2021. During this time period, the highest peak recorded is 109,000 users on Tuesdays at 9AM.

4.4.1. DepEd Commons Guest Access

Guests or unregistered users have view and download access to learning resources. Although not required to undergo user authentication, guest users are required to select their school affiliation and input their names. This is minimally required for statistical purposes.

Guest users, whether a student or a teacher, do not have access to the feedback or rating feature of learning resources.

4.4.2. Registered Student Access (https://commons.deped.gov.ph/students/sign_in)

a. There are student accounts that are preapproved. The list is provided by DepEd ICTS list which INTELIMINA migrated to the DepEd Commons database. Preapproved accounts receive an activation link on the provided emails. Students can then create their own DepEd Commons password and use this to login.

b. Use Sign in with Microsoft and student can access DepEd Commons using one's own O365 password. Email to be used though should be student's official DepEd O365 account.

4.4.3. Registered Teacher Access (https://commons.deped.gov.ph/accounts/sign_in)

a. There are teacher accounts that are preapproved. The list is provided by DepEd ICTS list which INTELIMINA migrated to the DepEd Commons database. Preapproved accounts receive an activation link on the provided emails. Teachers (and DepEd personnels) can then create their own DepEd Commons password and use this to login.

b. Use Sign in with Microsoft or Sign in with Google and users can access DepEd Commons using one's own O365 or GSuite/Google password. Email to be used though should be user's official DepEd O365 or GSuite/Google account.

4.4.4. Admin User Access (https://commons.deped.gov.ph/admin)

a. Superadmin. Only superadmins can create another superadmin and sub-admin accounts such as CO admin user, DITO admin user, and CI Approver admin user.

b. Sub-admin. CO and DITO admin users are preapproved accounts and can only be created via the Admin portal by a superadmin.

4.4.5. Approver Access (https://commons.deped.gov.ph/approvers/sign_in)

Only superadmins can create an Approver account. They are also preapproved and can only be created via the Admin portal by a superadmin.

4.4.6. Uploader Access (https://commons.deped.gov.ph/uploaders/sign_in)

Only superadmins can create an Approver account. They are also preapproved and can only be created via the Admin portal by a superadmin.

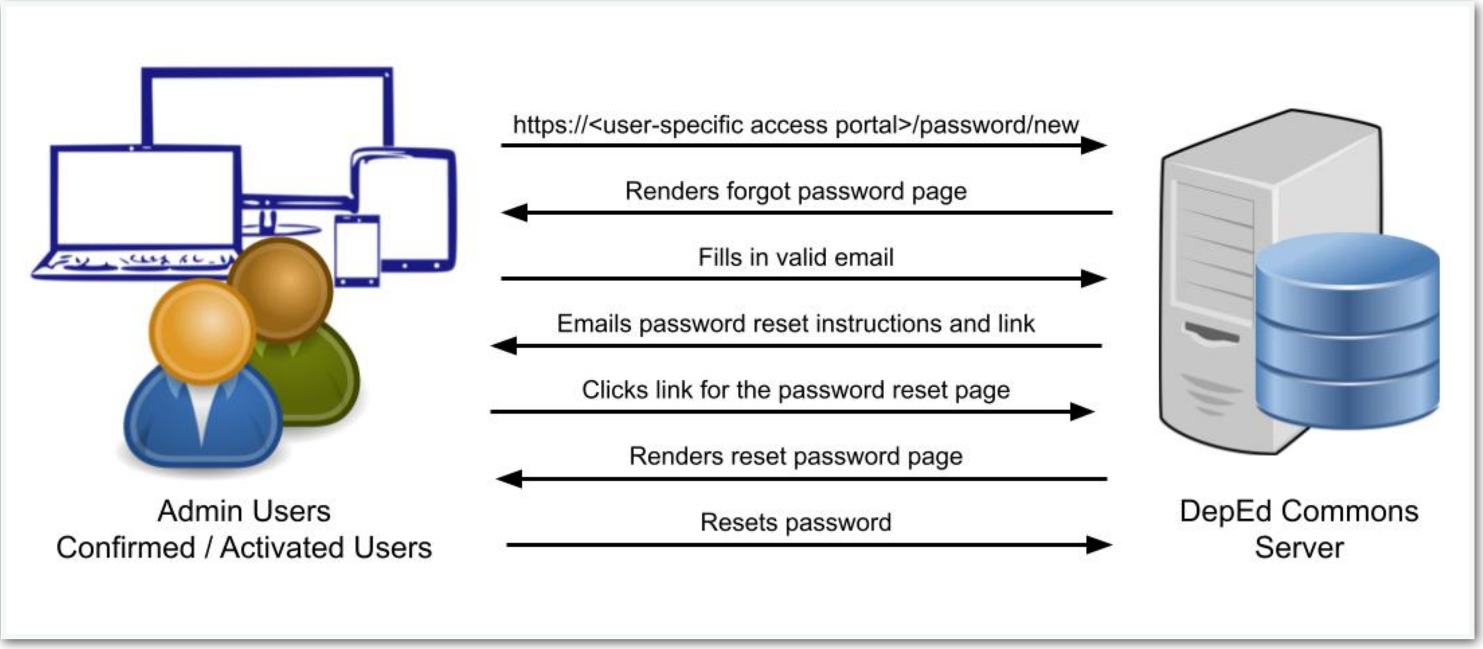

https://<user-specific access portal>/password/new
Renders forgot password page
Fills in valid email
Emails password reset instructions and link
Clicks link for the password reset page
Renders reset password page
Resets password
Admin Users
Confirmed / Activated Users
DepEd Commons
Server

Fig. 6. Self-Service Credentials Recovery Workflow - All Users

5. Standards and Policies

5.1. Credentials and Password

5.1.1. Password Expiration

Password expiration and composition can be configured in DepEd Commons. Currently, only idle session timeout for admin users is set (15 minutes). As such, the following are herein specified and recommended for security:

a. Enforce a change password policy every 90 to 180 days or twice a year, where the three recent passwords should not be used.

b. Enforce password composition that determines minimum length, special character inclusion, number inclusion, capitalized letter inclusion, etc.

5.1.2. Self-Service Credentials Recovery

Admin accounts and user accounts that were confirmed and activated can utilize the password recovery facility.

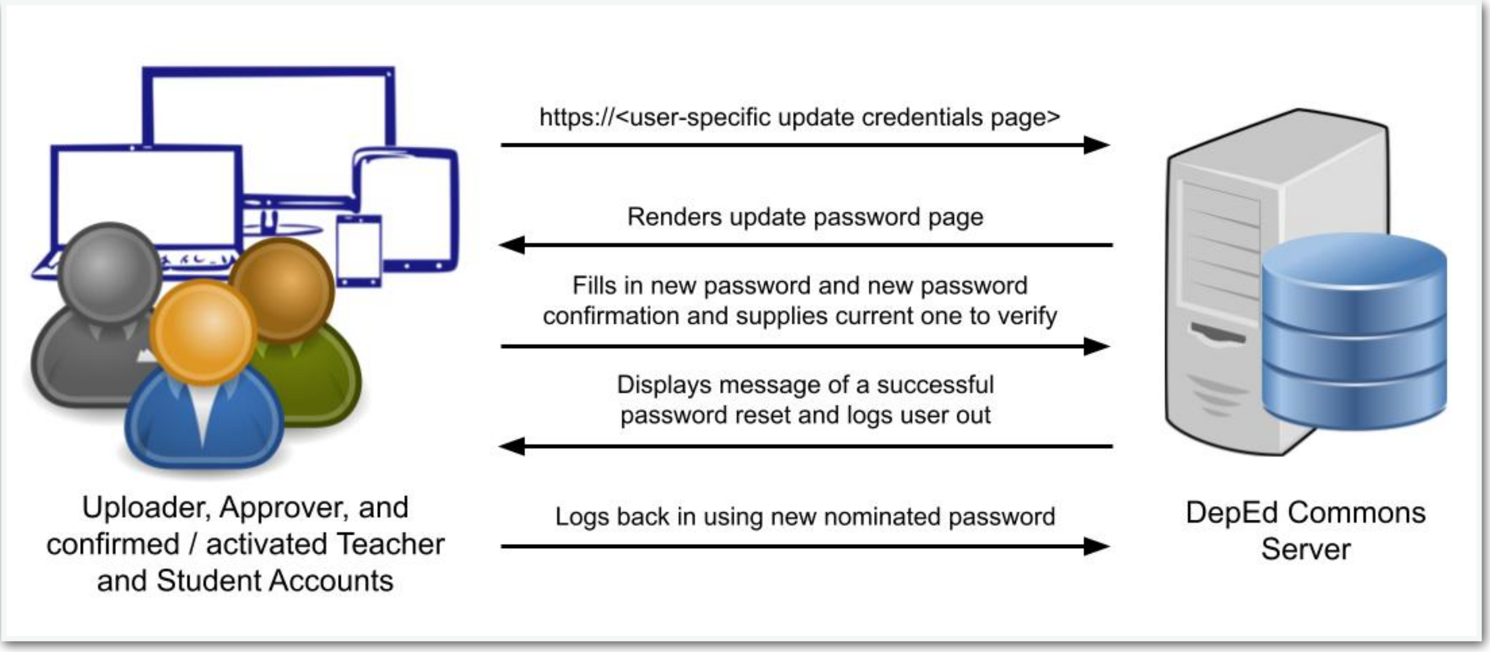

https://<user-specific update credentials page>
Renders update password page
Fills in new password and new password confirmation and supplies current one to verify
Displays message of a successful password reset and logs user out
Logs back in using new nominated password
Uploader, Approver, and confirmed / activated Teacher and Student Accounts
DepEd Commons Server

Fig. 7. Self-Service Credentials Reset Workflow for Uploaders, Approvers, Teachers, and Students

This is accessed by clicking the **Forgot your password?** link on the user's login portal and fills out required detail. The system then sends the instructions on the user's registered email address. *(See Fig. 6)*

5.1.3. Self-Service Credentials Reset

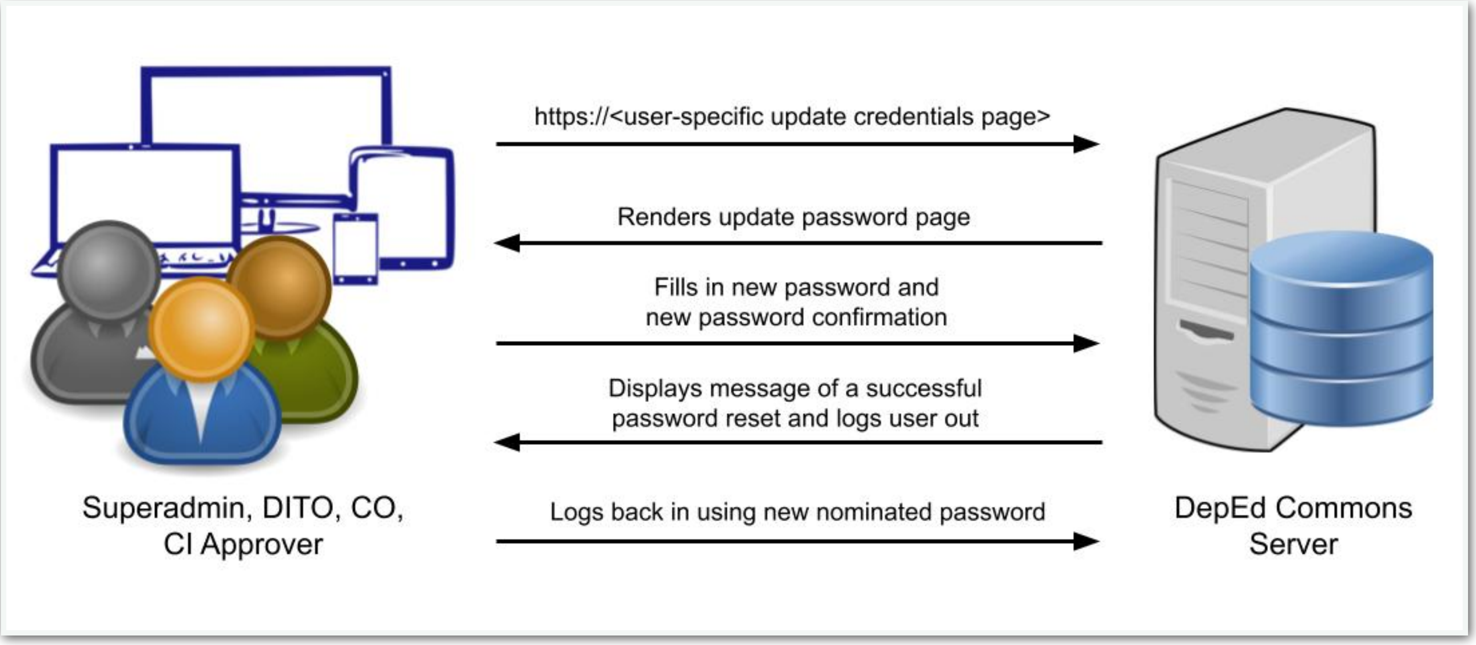

https://<user-specific update credentials page>
Renders update password page
Fills in new password and new password confirmation
Displays message of a successful password reset and logs user out
Logs back in using new nominated password
Superadmin, DITO, CO, CI Approver
DepEd Commons Server

Fig. 8. Self-Service Credentials Reset Workflow for Superadmin, DITO, CO, and CI Approver users

Self-service credentials reset facility is available only to Uploaders, Approvers, and confirmed and activated Student and Teacher Accounts. This is done by going to the **Edit Account > Credentials** page. User needs to supply nominated new password twice and current password to successfully reset or update own password. *(See Fig. 7)*

DITO, CO, CI Approver, and Superadmin users need to login to their accounts, go to **Profile > Edit Admin User** and supply the nominated new password twice.

5.2. Compliance with Data Privacy Act

Data protection, confidentiality, and governance are important elements entailed in each and every endeavor of Intelimina. We consider these crucial to our business and impose on ourselves several methods to ensure security, confidentiality, and integrity in processing of data and information, including personal information.

The Data Privacy Act or RA 10173 is overall intended to protect the integrity and confidentiality of personal data. As compliance, and to wit: “The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
Personal information must, be:

a. Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

b. Processed fairly and lawfully;

c. Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

d. Adequate and not excessive in relation to the purposes for which they are collected and processed;

e. Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and,

f. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing."[11]

DepEd Commons' compliance to the DPA is also available at https://commons.deped.gov.ph/privacy_policy.

6. Key Personnel and Support Staff

6.1. Specific to this project, the following key persons make up the Project Directory:

Name	Title / Organization	Email / Phone
Abram YC Abanil	Project Proponent - Project Head - End-user Unit (ICTS - DepEd)	abram.abanil@deped.gov.ph
Maria Clarisse Ligunas	Project Proponent - Technical Liaison (ICTS - DepEd)	mariaclarisse.ligunas@deped.gov.ph
Deng Silorio	Project Manager (Intelimina)	deng@intelimina.com, 09988506685
Jesse Nikko Ramos	Project Coordinator (Intelimina)	jepy@intelimina.com, 09291993302
Rystraum Gamonez	Technical Lead - SysAd (Intelimina)	rys@intelimina.com, 09175681889
John Philip Dorado	Technical Lead - Web & App Admin (Intelimina)	jp@intelimina.com, 09178662219
Jaja del Rosario	Helpdesk - User Support (Intelimina)	jaja@intelimina.com, 09088187502

6.2. The following channels are available for user support and issue resolution:

6.2.1. Email, 24/7: deped-support@intelimina.com
When submitting a request for support to deped-support@intelimina.com, a ticket is automatically generated in OSTicket, the support ticketing system for DepEd Commons and DepEd Mobile App.

[11] Republic Act No. 10173 - Data Privacy Act of 2012, Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Philippines], 12 August 2012. Retrieved on 25 May 2021 at https://www.privacy.gov.ph/data-privacy-act/.

6.2.2. Email and Phone, as per SLA coverage under Level of Escalation. The provision of these main contact persons still require reporters to submit a support request to deped-support@intelimina.com for proper issue tracking.

- Tier 1 - Level 4 incidents and errors (user inquiries)
  jaja@intelimina.com, 09088187502 - Jaja del Rosario
- Tier 2 - Levels 2 & 3 incidents and errors (application)
  jp@intelimina.com, 09178662219 - John Philip Dorado
- Tier 3 - Level 1 incidents and errors (server and database)
  rystraum@intelimina.com, 09175681889 - Rystraum Gamonez

APPENDIX A

Web Application Security Policy[12]

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within Intelimina Systems, Inc. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of INTELIMINA services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at INTELIMINA.

All web application security assessments will be performed by delegated security personnel either employed or contracted by INTELIMINA. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of INTELIMINA is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping

[12] This policy is based on the Web Application Security Policy created by and for SANS Institute for the Internet community.

phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1. Web applications are subject to security assessments based on the following criteria:

4.1.1. New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

4.1.2. Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

4.1.3. Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

4.1.4. Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

4.1.5. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

4.2.1. High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

4.2.2. Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

4.2.3. Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3. The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

4.3.1. Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

4.3.2. Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

4.3.3. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4. The tools and/or techniques that may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

5. 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.

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

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

Appendix B

Server Security Policy[13]

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by INTELIMINA. Effective implementation of this policy will minimize unauthorized access to INTELIMINA proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at INTELIMINA must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by INTELIMINA or registered under an INTELIMINA-owned internal network domain.

This policy specifies requirements for equipment on the internal INTELIMINA network.

4. Policy

4.1. General Requirements

4.1.1. All internal servers deployed at INTELIMINA must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based

[13] This policy is based on the Server Security Policy created by and for SANS Institute for the Internet community.

on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- ◉ Servers must be properly recorded and accounted in the Data Asset Monitoring. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact;
    - Hardware and Operating System/Version; and,
    - Main functions and applications.
- ◉ Information in the corporate enterprise management system must be kept up-to-date.
- ◉ Configuration changes for production servers must follow the appropriate change management procedures

4.1.2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

4.2. Configuration Requirements

4.2.1. Operating System configuration should be in accordance with approved InfoSec guidelines.

4.2.2. Services and applications that will not be used must be disabled where practical.

4.2.3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5. Trust relationships between systems are a security risk, and their use should be avoided.

Do not use a trust relationship when some other method of communication is sufficient.

4.2.6. Always use standard security principles of least required access to perform a function.

Do not use root when a non-privileged account will do.

4.2.7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

4.2.8. Servers should be physically located in an access-controlled environment.

4.2.9. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3. Monitoring

4.3.1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security- related events include, but are not limited to:

- Port-scan attacks;
- Evidence of unauthorized access to privileged accounts;
- Anomalous occurrences that are not related to specific applications on the host.

5. 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.

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

APPENDIX C

Database Credentials Coding Policy[14]

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of INTELIMINA's networks.

Software applications running on INTELIMINA's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the INTELIMINA Network. This policy applies to all software (programs, modules, libraries or APIS that will access a INTELIMINA, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don’t always use sanitized information.

4. Policy

4.1. General Requirements. In order to maintain the security of

[14] This policy is based on the Database Credentials Coding Policy created by and for SANS Institute for the Internet community.

INTELIMINA's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

4.2. Specific Requirements

4.2.1. Storage of Data Base User Names and Passwords

- ◉ Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
- ◉ Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- ◉ Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- ◉ Database credentials may not reside in the documents tree of a web server.
- ◉ Pass through authentication must not allow access to the database based solely upon a remote user’s authentication on the remote host.
- ◉ Passwords or pass phrases used to access a database must adhere to the minimum standards.

4.2.2. Retrieval of Database User Names and Passwords

- ◉ If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

4.2.3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed as regularly enforced. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

5. 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.

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

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with INTELIMINA.

Any program code or application that is found to violate this policy must be remediated within a 90-day period.

APPENDIX D

Remote Access Policy[15]

1. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of INTELIMINA, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to INTELIMINA's network from any host. These rules and requirements are designed to minimize the potential exposure to INTELIMINA from damages which may result from unauthorized use of INTELIMINA resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical INTELIMINA internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all INTELIMINA employees, contractors, vendors and agents with a INTELIMINA-owned or personally-owned computer or workstation used to connect to the INTELIMINA network. This policy applies to remote access connections used to do work on behalf of INTELIMINA, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to INTELIMINA networks.

[15] This policy is based on the Remote Access Policy created by and for SANS Institute for the Internet community.

4. Policy

It is the responsibility of INTELIMINA employees, contractors, vendors and agents with remote access privileges to INTELIMINA's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to INTELIMINA.

General access to the Internet for recreational use through the INTELIMINA network is strictly limited to INTELIMINA employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the INTELIMINA network from a personal computer, Authorized Users are responsible for preventing access to any INTELIMINA computer resources or data by non-Authorized Users. Performance of illegal activities through the INTELIMINA network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use INTELIMINA networks to access the Internet for outside business interests.

4.1. Requirements.

4.1.1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong pass-phrases.

4.1.2. Authorized Users shall protect their login and password, even from family members.

4.1.3. While using a INTELIMINA-owned computer to remotely connect to INTELIMINA's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4. Use of external resources to conduct INTELIMINA business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.5. All hosts that are connected to INTELIMINA internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as may be stated in the entered contracts.

4.1.6. Personal equipment used to connect to INTELIMINA's networks must meet the requirements of INTELIMINA-owned equipment for remote access.

5. 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.

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