ENEJDA DOKO **BINF3**

DATE: 15 April 2020

Non-functional requirements
Legislative and Accounting Requirements

Requirements are defined under full conviction to legislative system of Albania

LAW Nr. 2/2017 FOR KIBERNETIC SECURITY

Pursuant to Articles 78 and 83, point 1 of the Constitution, upon the proposal of the Council of Ministers,

This law applies to communication networks and information systems, the violation or destruction of which would affect health, safety, economic well-being of citizens and the effective functioning of the economy in the Republic of Albania. The processing of personal data, in order to implement this law, must be carried out in accordance with the provisions of **law no. 9887, dated 10.3.2008**, "**On the protection of personal data**", as amended.

According to LAW Nr. 8438, dated 28.12.1998 ABOUT TAXATION ON INCOME amended

Minimum wage decided 26000 decided in 2019.

Albania makes use of three-bracket progressive income;for income in range (0-30000 lek) 0% taxation,(30001-150000) 13% taxation;more than 150000 ,23 % taxation.

In addition to this we will take into account TVSH or VAT(Value added tax) which has value of 20%.

Social security and health contributions are taken into consideration.

Social security tax which is 11.2 % from employee contribution, 16.7% for employer ,23% for self-employed.Health contribution is 1.7% for both employer and employee,3.4 % for self-employed.

Security should be integrated at the earlier stage of lifecycle of the software instead of doing it later, which will reduce cost and risk of redesigning the software all over again.

1. Core Security Requirement

C.I.A. Triad [Confidentiality, Integrity and Availability] & A.A.A. [Authentication, Authorization and Accountability]

Confidentiality:

-protection against Disclosure of Sensitive Data to Unauthorized Individuals.

-ensure confidentiality when Data is at Rest, In-Transit and also when it is processed.

-Processes like Encryption, Steganography, Masking etc assist in assuring Data and Process Confidentiality.

Security Checklist should contain specifications required to implement these like, Protocols to Use, Encryption Strength, usage of Processes ensuring confidentiality like Random Number Generator etc

Integrity:

-ensure Reliability and Accuracy of the information.

-checking software functionality

-handled data is Complete and consistent.

Implementation of Security Controls like Hashing, Digital Signatures assist in ensuring Integrity. Specifications like Protocols, Data Randomness Strength (e.g. Salt Length) etc

Availability:

Availability Requirements ensures protection against unwanted destruction or disruption of Service. These are tricky requirements and should be captured as a part of Service Level Agreement (SLA) components like measurement of Maximum Tolerable Downtime [MTD] and Recovery Time Objective [RTO]. Requirement sheet should also contain measures to define and analyses Business Stress Analysis [BIA]. These measures should be in both Quantitative (Cost to Fix/Restore, Legal Obligations etc) and Qualitative (Reputation Loss).

Authentication and Authorization:

The system must control user access via an authentication mechanism based on a unique username and password login for each user

System Administrator specifies the minimum password length and whether passwords are case sensitive or not.

-Password must display an asterisk (*) or similar character

-legitimacy and validity of the Identity.

-permissions to be assigned to All Authenticated entities.

-changing password by entering a special code of company

-checking that the data is modified by authorized person in authorized manner

Accountability:

The system must log user access (including reporting): • date last used • unsuccessful log-in attempts (user name, password and workstation) log activity

-building record of user action and act as Detective Control

-detecting when Unauthorized User makes a Change, or when an Authorized User makes an unauthorized change.

General (Application) Security Requirements

From Application/Software Security prospect, General security requirements should capture proper Session, Error and Configuration management needs.

Session Management:

Product Security requirement sheet should capture methods and measures required to Secure Sessions. Requirements defining Uniqueness and Randomness of Session (Non-Guessable), Expiry, Non-reusability etc should be defined.

Error Management:

-avoid Disclosure Threats like revealing of any Internal Application architecture, Design and Configuration Information.

Configuration management:

-avoid any Sensitive Data

Measure to take: **Initialization and Disposal of Global Variables**, **Hashing/Encryption of Sensitive data**

3. Operational Security Requirements

Once Application/Software is developed and deployed, Security should also be considered when it is Operational in environment to avoid any unwanted disclosure or leakage.

Deployment Environment:

Security Requirement list should capture information about environment in which Software will be deployed and who will be using same. Environment Compliances and Industry Standard requirements are driven with this information.

Archiving:

-capture archiving requirements to comply with organization's policy and regulations.

Measures like Where (media type) and How (online/offline, format, encryption) Data will be stored, Data retrieval policy etc

Anti-Piracy:

-part of Commercial off-the-shelf (COTS) requirement.

It includes Code Obfuscation, Signing, Anti Tampering, Licensing, IP Protection mechanism.

International Regulation:

International Regulation and Compliance needs should also be discussed and captured as a part of Security Requirement Gathering.

1. Secure Password Storage

Password encryption

-MD5 and other standard hashing algorithms are known techniques

Salting is one of the coding techniques that support prevent password hashes de-duplication, but this alone isn't enough.

For storing the password, we recommend combining three major techniques including one-way algorithm, salt and an algorithm, which is intentionally slow, for avoiding GPU cracking rigs (which allows the attackers to execute 25 million attempts to crack the password) and similar resources from stealing the passwords.

-PBKDF2 and SCRYPT are the excellent algorithms that can be utilized to store the password

2. Query Parameterization

Query parameterization to avoid SQL injection.

3. Appropriate Output Encoding To Prevent XSS

Conceptual output **escaping/encoding** programming method need to follow in order to stop XSS (Cross Site Scripting) attacks used for executing the site defacement, session hijacking, network scanning, site phishing/redirection, undermining CSRF defenses, data theft, keystroke logging and much more

4. Content Security Policy

Entire JavaScript deployed in the separate JavaScript file externally to detect malicious JavaScript in HTML document and reject the action.

5. Defending Cross Site Request Forgery

This attack involves tricking the user who logged into an authenticated site to perform a malicious action.

-deploying cryptographic tokens. In addition, requiring the user to re-authenticate in order to finish an event or transaction for avoiding in-session hijacks.

6. Multi Factor Authentication

-multi-factor authentication solutions to enhance the security.

7. Security Design For Forgotten Password

A stronger process for requesting a new or existing password should include:

- Validate user identity via security questions
- Send a randomly generated token to the user through out-of-band method
- Validate code in the current web session and apply a lockout policy
- Change the password

8. Proper Error Handling

-configuring the server differently in the development environment and production environment to hide the errors when making the application accessible to the end users

9.Control Access

The system should allow for each user to be assigned to a user group; for example by job function or departmental structure/hierarchy.

The system must not display any function or information to which the user has not been granted access:

Accounting principles

All action will be complying standards of **Internal Auditing Standards Board (IASB)** and **Information Systems Audit and Control Association** (**ISACA**) issues .

TRANSACTION PROCESSING

-Narrative can be attached to any transaction or transaction line.
-handle all transactions in different currencies.

-the authorized user/s can amend or cancel (delete or void) any transaction at any time prior to authorization or the commitment of data to the database, subject to process and user access controls.

-identify elements which are for expenditure and income (operating statement items) and for assets and liabilities (balance sheet items).

The financial functionality of the overall system.

-a section in which income, expenditure or activity is to be recorded
reflecting what expenditure has been incurred, income received, balance sheet accounts etc

-When required, the application of changes must be from a specific effective date within the financial year. In particular, audit trails of previous data entry and processing should remain intact. All such adjustments must be also applied to the current year where relevant.
-Re-calculations performed after posting adjustments have been made.

ACCOUNTING PERIODS

The system should allow at least 53 periods to be defined for each individual entity; for example: • 52 or 53 weeks • 12 calendar months • 12 periods based on 4, 4 and 5 weeks • 13 periods based on 4 weeks or The system should allow the addition of additional periods if required for year-end purposes.

-periods can not be deleted once data has been posted to them.
-multiple years can be open at the same time though posting for ordinary users will only be possible in the current year.

-closing balances from one period must be rolled into the opening balances for the subsequent period(s).

The system must warn the user if they attempt to post to a non-current period.

DATA ENTRY, VALIDATION, LOOKUP

-automatic validation during data entry
-not allowing final posting of entries until the relevant validation checks have been performed.

-Support drop down list of all matching entries with facilities to allow the user to identify and select the required entry; for example, a list of creditors and their addresses.

-provide input controls: • data type; • minimum field size • within range/outside limits; for example valid day within month • inappropriate punctuation; for example, inappropriate characters in monetary values • relationship with other fields; for example, start/end dates

-duplicate invoice checking to prevent entry of duplicate invoices • warn the user before allowing the duplication of invoices

-workflow type functionality for example, create a transaction on a specific date or after a specified interval, or send an email if a specified balance/value is exceeded etc.

Audit Log

The system should allow the audit report to be: • displayed on screen • printed to hardcopy output •saved to electronic output; for example. ASCII, RTF, PDF file

System Integrity

The system must provide transaction data integrity facilities including: • reconciliation of control accounts to subsidiary ledgers • maintaining the General Ledger in balance • reconciliation of General Ledger transactions to balances • reconciliation of Accounts Payable transactions to supplier balances • reconciliation of Accounts Receivable transactions to customer balances • reconciliation of Fixed Assets to asset control accounts

Archiving

-all data can be archived and re-accessed any time

GENERAL LEDGER

-fully integrated or fully interfaced with Accounts Payable, Accounts Receivable, Cash Book and Fixed Assets.

-maintain self balancing ledgers.
-allow the definition of multiple VAT rates; for example, standard, zero-rated, exempt, non-recoverable

JOURNALS

The system must allow the entry and posting of journals as a two stage process comprising (1) input of the entry and (2) its checking, amending, and authorization which will lead to the automatic updating of the General Ledger with no further intervention required.

PERIOD END PROCESSING

- automatic checks that all batch interface routines have been executed • reversal of accruals • update of monthly transaction records • preparation of full period audit trail • standard monthly journals processing

YEAR END PROCESSING

The system must allow year-end adjustments in the General Ledger after the Accounts Payable and Accounts Receivable Ledgers have been closed for the year

BUDGET MANAGEMENT

-fully integrated or fully interfaced budgeting and forecasting functionality.
-support budgeting against both financial and statistical entries.
The system should allow budget information to be exported in the following formats: • Microsoft Access • Microsoft Excel • XML • CSV, ASCII text file etc.

CASH MANAGEMENT

The system's cash book facility must be fully integrated or fully interfaced with the General Ledger, Expenses Claims, Petty Cash, Accounts Payable and Accounts Receivable.

The system should have the ability to manage multiple petty cash accounts and their associated control accounts.

-must be able to correctly handle VAT.

BANK RECONCILIATION

The system should provide the ability to load the bank statement and auto reconcile in one step.