Network and Information Security Management

Team 3 Design Document

8 January 2022

Team Members

Name	ePortfolio
Andrey Smirnov	https://soundmaven.github.io/e-portfolio/
Michael Justus	https://micjustus.github.io/essex-eport2/
Taylor Edgell	https://tedgell.github.io/MSc-ComputerScience/
Grace Clarke	https://gclarke95.github.io/University/

Document Version History

Version	Date	Author	Details
0.1	25/11/21	Taylor Edgell	Document creation
0.2	04/12/21	Taylor Edgell	Website Considerations
0.3	06/12/21	Andrey Smirnov	Vulnerabilities
0.4	07/12/21	Grace Clarke	Governing Bodies & Regulations
0.5	07/12/21	Michael Justus	Review. Mitigations and Recommendations based on theoretical assessments
0.6	13/12/21	Michael Justus	Review. Additional recommendations and references
0.7	13/12/21	Andrey Smirnov	New GDPR compliance table in the vulnerabilities section
0.8	13/12/21	Grace Clarke	Updating Governing Bodies & Assumptions
0.9	15/12/21	Taylor Edgell	Edits and amendments
0.10	15/12/21	Andrey Smirnov	Minor amendments
0.11	16/12/21	Michael Justus	Updates to recommendations and risks.
0.12	18/12/21	Michael Justus	Reduce word count for recommendations. Add a “Tools” column.
0.13	18/12/21	Taylor Edgell	Reduction and Edits
0.14	18/12/21	Andrey Smirnov	More reduction. Formatted list of references

0.15	19/12/21	Michael Justus	Review
0.16	19/12/21	Grace Clarke	Project Timeline. Formatting and Edits
0.17	19/12/21	Taylor Edgell	Final review
1.0	20/12/21	Taylor Edgell	Submission

Definitions and Abbreviations

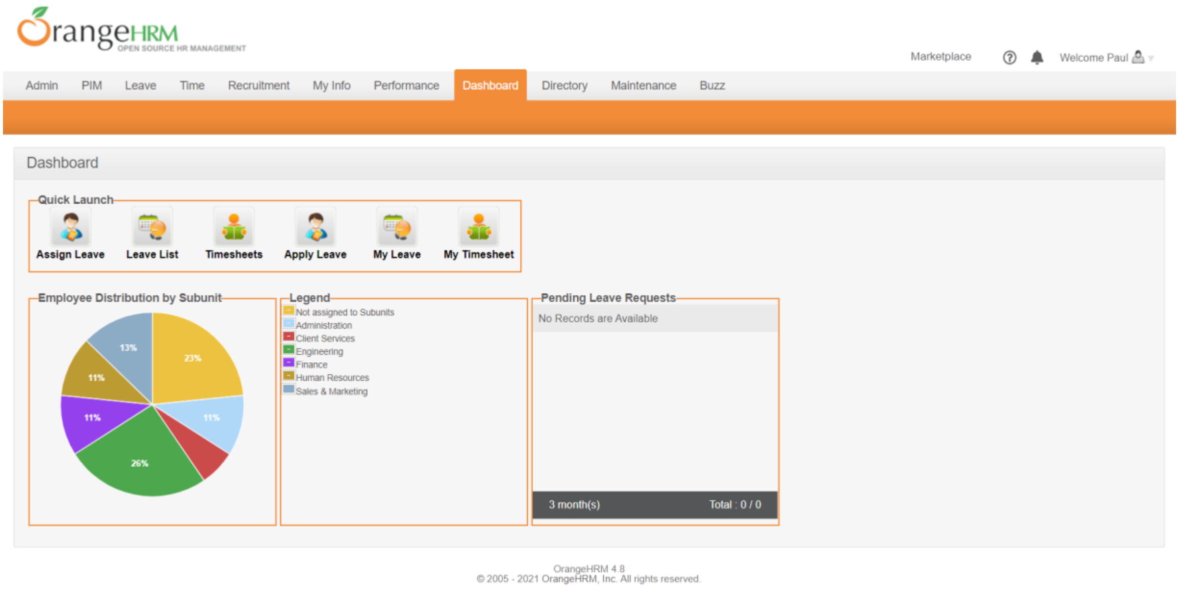
Acronym	Description
2FA	Two-factor authentication
AD	Active Directory
BYOD	Bring Your Own Device
CIPD	Chartered Institute of Professional Development
CVE	Common Vulnerability and Exploits
CVSS	Common Vulnerability Scoring System
EU	European Union
GDPR	General Data Protection Regulation
GNU	GNU Is not Unix
HR	Human Resources
HRM	Human Resources Management
NVD	National Vulnerability Database
PII	Personally Identifiable Information
SHRM	Society for Human Resource Management
UK	United Kingdom

Word Count (Excluding titles and captions): **1054**

Contents

1. Overview

The website for assessment is https://staffmatters.co.uk/, an open-source human resources (HR) management system allowing several people to access, contribute, and share stored data (Singhal et al., 2010).



No Records are Available

3 month(s) Total : 0 / 0

OrangeHRM 4.8
© 2005 - 2021 OrangeHRM, Inc. All rights reserved.

Figure 1 Website dashboard

2. Assumptions

- The website has a UK domain; therefore, consideration is given only to UK regulatory and governing bodies.
- No context is provided regarding environment, registrar, host etc. This information will only be evaluated at surface level.
- CIPD and SHRM are referenced in this report. Whilst not applicable as legal governing bodies, they require members to uphold industry and government standards within the HR profession.
- OrangeHRM is not classified as an e-commerce site and therefore, WebTrust and SysTrust Service Principles are not considered.

3. Governing Bodies and Regulations

3.1 Governing Bodies

The Information Commissioner's Office (ICO) is a UK public, independent authority that regulates, promotes, and enforces the UK's GDPR data protection. The Chartered Institute for Professional Development (CIPD) is a professional body which accredits and awards HR qualifications that are recognised for meeting professional standards within the UK. The Society for Human Resource Management (SHRM) is the largest global HR professional organisation that provide regular updates on legislative news and HR policy documents for use in the workplace.

3.2 Regulations

The following regulations are applicable to OrangeHRM:

- Data Protection Act 2018 (DPA)
- General Data Protection Regulation (UK GDPR)
- Employment Law

The 2018 DPA states that anybody responsible for personal data must follow the data protection principles as illustrated in **Error! Reference source not found.**.

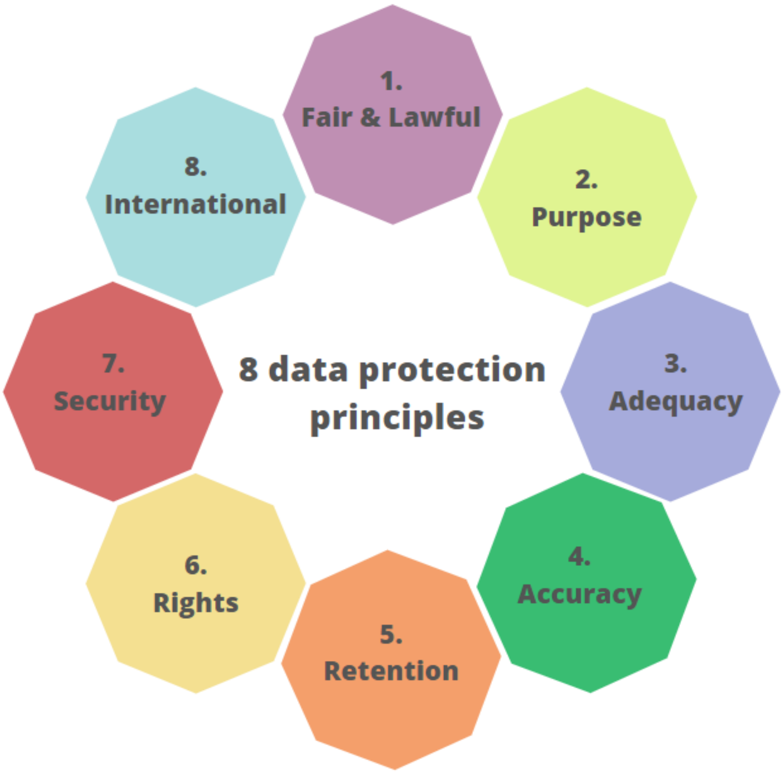


Figure 2 Data protection principles

Organisations have an obligation to ensure that data contained within the HR product is appropriately secured ensuring sufficient protection against unlawful or unauthorised processing, access, loss, destruction, or damage (UK GOV, 2018). HR data must be reviewed periodically and erased (or anonymised) when such data is no longer needed (Woska, 2013). Failure to ensure data is secure means organisations may not be compliant with UK employment law.

4. Website Considerations

4.1 Audience and Industry

HR systems allow companies to “alter habits and routines that treat economic, social and environmental performance as competing goals” (Ren & Jackson, 2020). Stakeholders of OrangeHRM are employees and employers (including company owners and shareholders). To a lesser degree, suppliers (reputation-wise) and the public also have an interest in how companies ethically treat their employees.

4.2 Held Information/Data

Employee data held by HR departments in the UK is considered confidential and must be protected according to GDPR. “Appropriate measures need to be taken to ensure the security of the data” (Regulation, GDP, 2018).

OrangeHRM’s data is primarily confidential employee information which includes:

- Employee name, contacts, addresses, and general details (sex, age, nationality, etc.)
- Bank details
- Position entitlements (Leave, Pension etc.)
- Salary
- Leave and timesheets
- Job description and expectations
- Qualifications and skills
- Open company positions
- KPI’s and performance reviews

4.3 Functionality

Table 1 Website functionalities

Functionality	Explanation
Leave management	• Manages statutory leave (UK GOV, 2021).
Employee Records	• Employee-specific details
Employee management	• Shift patterns • Payroll • Attendance
Recruitment	• Open positions • Applicants
Performance Review	• Yearly targets and reviews
Contact Information	• Organisations contact directory
User management	• User credentials

5. Vulnerabilities

5.1 Threat Analysis Framework – OWASP TOP 10

Table 1 Vulnerabilities per OWASP framework

OWASP Category	Potential OrangeHRM vulnerability
A01 – Injection	• Lack of input validation.
A02 – Broken Authentication	• Weak authentication mechanisms.
A03 – Sensitive Data Exposure	• Insufficient database security. • Poor data backup strategy.
A04 – *XML External entities**	
A05 – Broken Access Control	• Inadequate access controls that allow access to restricted data by unauthorised users
A06 – Security Misconfiguration	• Lack of proper environmental controls.
A07 – *Cross-Site Scripting XSS**	
A08 – *Insecure Deserialization**	
A09 – Using components with known vulnerabilities	• Irregular vulnerability upgrades in the hosted environment.
A10 – *Insufficient logging and monitoring**	

** Considered to be out of scope of assignment.*

5.2 Data security

OrangeHRM might be vulnerable to data privacy and security breaches that can occur due to insufficient data security controls, both in the hosted environment and at the application level (Ediriweera, 2021).

5.3 Open-source security

OrangeHRM is free software distributed under the GNU General Public License. There are certain security challenges associated with adopting this specific type of software (Williams, 2020):

- Code is maintained in a *public repository*. Vulnerabilities are shared with the project's community before they are reported to organisations such as OWASP or disclosed to NVD, NVE or CVSS.
- Open-source software may use difficult to track *vulnerable or outdated components*. OWASP Top 10 documents this in the sixth category for awareness (OWASP Foundation, 2021).
- Transitive or *nested dependencies* often introduce risks inherited by applications that rely on third-party components (Springett, N.D.).

5.4 GDPR compliance

In their research regarding the impacts of GDPR on HR systems, Goncalves et al. (2020), elicited requirements that specify the operation of software compliant with GDPR (shown in Table 3):

Table 3 GDPR compliance requirements

Requirement	**Type**
A login screen is available to authenticate users.	Functional
The authorisation level permits viewing, editing, and removing employees and other sensitive information.	Functional
Data Owners can view and correct their personal information.	Functional
Log files containing records of all activities are available for Data Protection Officers to view.	Functional
Data security is enforced through character masking and encrypting PII in the database.	Non-functional
The system uses firewalls and up-to-date antivirus software, safe network communication uses TLS/SSL protocol.	Non-functional
Two-factor authentication (2FA) protects user access.	Non-functional
The system performs automatic data backups.	Non-functional

6. Recommendations, Mitigations and Tools

6.1 Business Risk Level: Severe

6.1.1 Vulnerability: Authentication

Table 4 Weak authentication

Risk	Recommendation
Passwords are weak.	• Implement password policy (e.g., length, complex characters, refresh interval)
Unauthorised users can access sensitive data.	• Apply code of conduct for users. • Sufficient training

6.1.2 Vulnerability: Security Access Controls

Table 5 Inadequate access controls

Risk	Recommendation
Ex-employees may still access the system.	• Revoke permissions and access rights of ex-employees

6.1.3 Vulnerability: Environmental Controls

Table 6 Environmental controls

Risk	Recommendation
Attachments contain malicious code.	• Scan all content received. • Implement a BYOD policy to scan personal devices for malicious code.
Brute force attacks against the system.	• Implement complex login requirements; two-factor authentication or Combination of passwords, biometric and facial recognition (Kennedy & Olmsted, 2017) • Account lockout policy.

6.1.4 Vulnerability: Data Privacy

Table 7 Data privacy

Risk	Recommendation
Lack of PII policy when operating within the EU and UK.	• Identify data that directly identifies an individual (Digital Guardian, 2017; GDPR, 2021).
Data in-transit is easily intercepted, read, or modified.	• Protect all endpoints with HTTPS and X509 certificates. • Leverage HSTS.

6.1.5 Vulnerability: Data Access Controls

Table 8 Access controls

Risk	Recommendation
Data storage has insufficient access controls in place.	• Assign roles and groups to every function in the system (Sandhu et al., 2000).

6.1.6 Vulnerability: Data Backups

Table 9 Data backups

Risk	Recommendation
Data backups and storage are not encrypted.	• Utilise AES to encrypt data backups (Pancholi & Patel, 2016).

6.2 Tools

Kali Linux will be our primary tool of choice, as it contains many pre-installed penetration tools vital to scanning our website. A break down is seen in Appendix B.

7. Summary

All researched information, including but not limited to regulations, site functionality, vulnerabilities, and mitigations, will be used to create the executive summary. Research into GDPR and HR data security regulations will be used to tailor scanning and vulnerability tests in the second half of the assignment.

Word Count (Excluding titles and captions): **1054**

References

Digital Guardian (2017) The Definitive Guide to Data Classification. Classification for Data Protection Success. Available from: https://infosecpartners.com/wp-content/uploads/2017/02/The-Definitive-Guide-to-Data-Classification.pdf [Accessed 12 December 2021].

Ediriweera, D. (2021) A Guide to Data Security in an HRIS. Available from: https://www.orangehrm.com/blog/a-guide-to-data-security-in-an-hris/ [Accessed 6 December 2021].

Foxall, D. (2021) Five basic HR data security threats in 2021. Available from: https://www.hrmsworld.com/hr-data-security-threats.html [Accessed 7 December 2021].

GDPR (2021) GDPR personal data – what information does this cover? Available from: https://www.gdpreu.org/the-regulation/key-concepts/personal-data/ [Accessed 12 December 2021].

Goncalves, E., Teixeira, P. & Silva, J. (2020) ‘Development of GDPR-Compliant Software: Document Management System for HR Department’, 15th Iberian Conference on Information Systems and Technologies (CISTI). Seville, 24-27 June. New York: IEEE. 1-6.

Kennedy, W. & Olmsted, A. (2017) ‘Three factor authentication’, *12th International Conference for Internet Technology and Secured Transactions (ICITST).* Cambridge, 11-14 December. New York: IEEE. 212-213.

OWASP Foundation (2021) A06:2021 – Vulnerable and Outdated Components. Available from: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ [Accessed 6 December 2021].

Pancholi, V. & Patel, B. (2016) Enhancement of cloud computing security with secure data storage using AES. *International Journal for Innovative Research in Science and Technology 2*(9): 18-21.

Regulation, GDP (2018) General data protection regulation (GDPR). Intersoft Consulting: 24(1).

Ren, S. & Jackson, S. (2020) HRM institutional entrepreneurship for sustainable business organisations. Human Resource Management Review 30(3): 100691.

Sandhu, R., Ferraiolo, D. & Kuhn, R. (2000) The NIST model for role-based access control: towards a unified standard. *ACM workshop on Role-based access control* 10(1): 344287-344301.

Singhal, N., Mohan, T. & Sarkar, S. (2010) A Comparative Study Based on Open Source Content Management Systems. *Indian Journal of Computer Science and Engineering* 1(4): 267-276.

Springett, S. (N.D.) Component Analysis. Available from: https://owasp.org/www-community/Component_Analysis [Accessed 6 December 2021].

UK GOV (2018) Data Protection. [online] gov.uk. Available from: https://www.gov.uk/data-protection [Accessed 4 December 2021].

UK GOV (2021) Holiday entitlement rights. Available from: https://www.gov.uk/holiday-entitlement-rights [Accessed 4 December 2021].

Williams, J. (2020) Removing a false sense of (open source) security. Computer Fraud & Security 6(1): 8-10.

Woska, W. (2013) Legal Issues for HR Professionals: Workplace Investigations, *Public Personnel Management* 42(1): 90-101.

8. Bibliography

Moores, T. & Dhillon, G. (2003) Do privacy seals in e-commerce really work? *Communications of the ACM* 46(12): 265-271.

National Cyber Security Centre (N.D.) Understanding vulnerabilities. Available from: https://www.ncsc.gov.uk/information/understanding-vulnerabilities [Accessed 6 December 2021].

Appendix A

Project Timeline

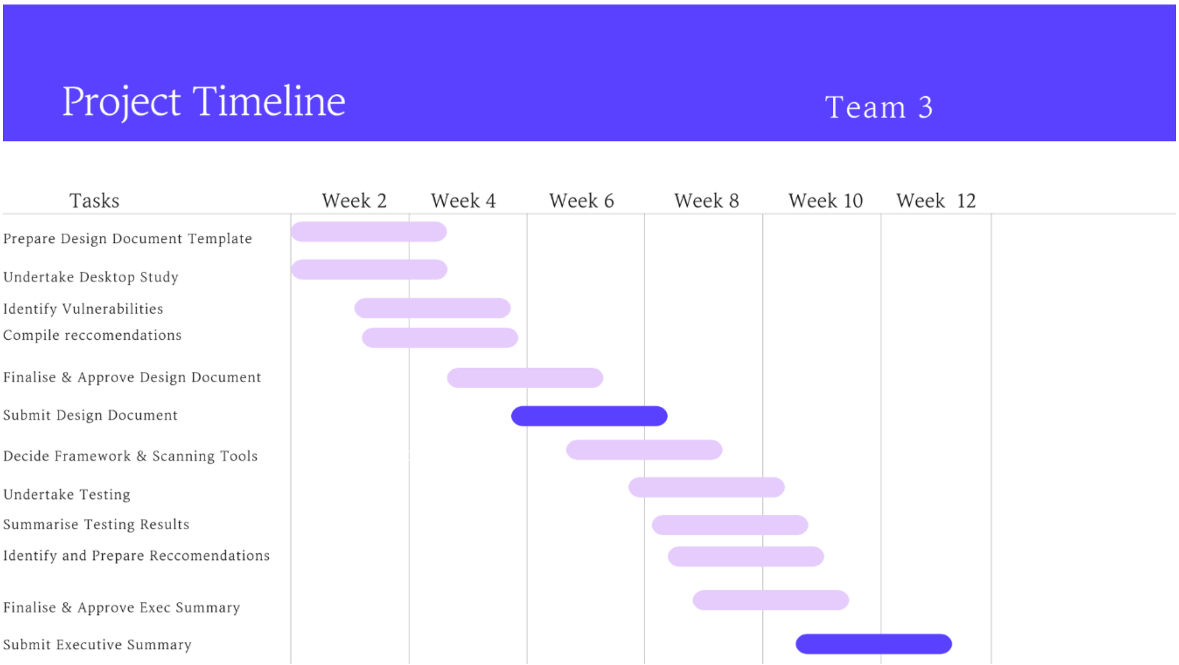


Figure 2 Network information security delivery timeline

Appendix B

Tool Analysis

Tool	Coverage
Kali Linux	All-encompassing security focused OS with many pre-installed penetration testing tools
SQLmap	Automated detection of SQL injection flaws
Nmap	Network exploration and security auditing
Metasploit	Includes a wide variety of modules including exploits, payloads, listeners, shellcode etc.