University of Plymouth

School of Engineering,

Computing, and Mathematics

COMP3000

Computing Project

2024/2025

Distributed Version Control System

Benjamin Sanders-Wyatt

10808929

BSc (Hons) Computer Science

Acknowledgements

Supervisors

Peers

Testers

Supporters

Abstract

(250-300 ~3%)

Stand alone summary

Background, aim, key objectives, methodology, major results, conclusions

Contents

[1 Introduction 4](#_Toc195313202)

[1.1 Project Context and Motivation 4](#_Toc195313203)

[1.2 Problem Statement 4](#_Toc195313204)

[1.3 Objectives 4](#_Toc195313205)

[1.4 Structure of the Report 4](#_Toc195313206)

[2 Background 4](#_Toc195313207)

[2.1 Enterprise needs 4](#_Toc195313208)

[2.2 Evolution of Version Control Systems 4](#_Toc195313209)

[2.3 Gaps 4](#_Toc195313210)

[3 Methodology 4](#_Toc195313211)

[3.1 Project Management 4](#_Toc195313212)

[3.1.1 Agile 4](#_Toc195313213)

[3.1.2 Tools 4](#_Toc195313214)

[3.2 Tools & Technologies 5](#_Toc195313215)

[4 Methodology & Implementation 5](#_Toc195313240)

[4.1 Software Development Lifecycle 5](#_Toc195313242)

[4.2 Tools & Technologies 5](#_Toc195313243)

[4.3 System Architecture & Design 5](#_Toc195313244)

[5 Legal, Social, Ethical, & Professional (LSEP) Issues 5](#_Toc195313245)

[5.1 Legal Considerations 5](#_Toc195313246)

[5.1.1 Data Protection & Privacy Compliance 5](#_Toc195313247)

[5.1.2 Secure Authentication & Account Management 5](#_Toc195313248)

[5.1.3 Licensing & Intellectual Property 6](#_Toc195313249)

[5.1.4 Audit & Accountability 6](#_Toc195313250)

[5.2 Social Considerations 6](#_Toc195313251)

[5.2.1 User Trust & Data Sovereignty 6](#_Toc195313252)

[5.2.2 Accessibility & Transparency 6](#_Toc195313253)

[5.3 Ethical Considerations 7](#_Toc195313254)

[5.3.1 Responsible Data Handling 7](#_Toc195313255)

[5.3.2 Automated systems 7](#_Toc195313256)

[5.3.3 Transparency in Operations 7](#_Toc195313257)

[5.4 Professional Considerations 7](#_Toc195313258)

[5.4.1 Adherence to Industry Standards 7](#_Toc195313259)

[5.4.2 Quality Assurance & Continuous Improvement 7](#_Toc195313260)

[5.4.3 Documentation 8](#_Toc195313261)

[5.4.4 Risk Management & Incident Response 8](#_Toc195313262)

[6 Project Management 8](#_Toc195313263)

[6.1 Planning & Scheduling 8](#_Toc195313264)

[6.2 Risk Management 8](#_Toc195313265)

[6.3 Tools & Techniques 8](#_Toc195313266)

[7 End-Project Report 8](#_Toc195313267)

[7.1 Evaluation of Objectives 8](#_Toc195313268)

[8 References 10](#_Toc195313269)

[9 Appendices 12](#_Toc195313270)

[9.1 User Guide 12](#_Toc195313271)

[9.1.1 Instillation Instructions 12](#_Toc195313272)

[9.1.2 Minimum System Requirements 12](#_Toc195313273)

[9.1.3 Usage Guide 12](#_Toc195313274)

[9.2 Project Management 12](#_Toc195313275)

WORD COUNT: **10000**

https://github.com/benjaminsanderswyatt/COMP3000-JanusVersionControl

# Introduction

## Project Context and Motivation

## Problem Statement

## Objectives

Functional and non functional requirements

## Structure of the Report

This report will

# Background

## Enterprise needs

## Evolution of Version Control Systems

Centralised systems

Distrubuted

## Gaps

# Methodology

## Project Management

### Agile

### Tools

## Tools & Technologies

# Methodology & Implementation

## Software Development Lifecycle

## Tools & Technologies

## System Architecture & Design

# Legal, Social, Ethical, & Professional (LSEP) Issues

Significant attention was given to ensuring that legal, social, ethical, and professional issues were addressed both in and before the development of Janus. This section evaluates the measures to manage these concerns and discusses their implications for system design and accountability.

## Legal Considerations

### Data Protection & Privacy Compliance

Janus is designed to operate entirely on-premise, ensuring that sensitive code and personal data remains within the organisation’s control. By leveraging Docker to deploy the system within a controlled subnet, the system minimises risks associated with external data exposure; this approach supports compliance with data protection regulations such as GDPR (European Union, 2016) and the Data Protection Act (UK Government, 2018).

Additionally, enforcing HTTPS for all data transfers provides an essential layer of encryption that safeguards data in transit and mitigates the risk of interception (OWASP, 2025).

### Secure Authentication & Account Management

Robust security is implemented using JSON Web Tokens (JWT) for API authentication, enabling secure communications between system components; this method is widely recognised for its efficiency in distributed environments (Jones, et al., 2015). The system utilises Personal Access Tokens (PAT) that are revocable and have configurable expiry times, reducing the reliance on static passwords and enhancing session security (National Instuture of Standards and Technology, 2017).

Furthermore, passwords are salted and hashed using industry-standard cryptographic practices (600,000 iterations of PBKDF2 with SHA256), ensuring resilience against brute force and dictionary attacks (OWASP, 2025). The use of 128-bit salt is balanced between collision risk and performance (NIST, 2017). These measures ensure that stored credentials are robust and that data integrity is maintained through transactional data interactions (Oracle, 2025).

### Licensing & Intellectual Property

Janus integrates various third-party libraries and frameworks, all of which have been reviewed for licensing compatibility; this minimises legal risks related to open-source or proprietary components (OSI, 2024).

In addition, Janus has plugin functionality that allows users to develop custom commands; this functionality is designed for user customisation of the system. As a result, the intellectual property of the custom-developed plugins will be held by the user or organisation (Svitla, 2024).

### Audit & Accountability

An essential component of Janus is its comprehensive audit logging, which records all database interactions to create a solid audit trail. This supports internal audits and serves as legal evidence in cases of data breaches or non-compliance; transparency in system operations is maintained because both the old and new states of data are logged, ensuring accountability and regulatory compliance (Souppaya & Kent, 2006).

## Social Considerations

### User Trust & Data Sovereignty

A key social advantage of Janus is the enhanced control organisations have over their codebases; by eliminating the need for external cloud services, user trust is improved as all information is managed internally. This approach not only reinforces data sovereignty but ensures that users know exactly who handles their information (Scherenberg, et al., 2024).

### Accessibility & Transparency

Janus has been designed with the user experience in mind. The React-based web interface adheres to most modern accessibility standards, such as the WCAG guidelines (WCAG, 2024), ensuring that users from any background can effectively navigate and utilise the system.

Clear documentation is provided, including detailed usage instructions for the CLI. While features like light/dark themes support usability by accommodating user preferences and reducing eye strain (Kristallovich & Eisfeld, 2020).

## Ethical Considerations

### Responsible Data Handling

Ethically, Janus prioritises the responsible management of user data. Users must accept the Terms of Use and Privacy Policy before creating an account, ensuring informed consent regarding data handling.

Sensitive data remains confined within the organisation, minimising the risk of unauthorised exposure; this approach not only protects individual privacy rights but also upholds ethical standards in data management (Chang, et al., 2016).

### Automated systems

Janus deliberately avoids automated resolutions, such as automated merge conflict handling, ensuring that users fully hold control over critical actions: this places accountability with the users and reduces the risk of compromising data integrity.

### Transparency in Operations

The detailed audit logging mechanism, combined with explicit Terms of Use and Privacy Policy, ensures that users are well informed about data collection and processing practices; the transparency is essential for ethical accountability and enabling users to make informed decisions about their data (ICO, 2025).

## Professional Considerations

### Adherence to Industry Standards

From a professional standpoint, Janus adheres to established industry best practices in software development. The implementation of design principles such as DRY (Don’t Repeat Yourself) (Thomas & Hunt, 2000) and the use of modular, reusable code components contribute to maintainability and scalability (Parnas, 1972). The selection of industry-standard frameworks, such as .NET Core and React, ensures that the system is robust and that professional standards are upheld (Anjum & Alam, 2019).

### Quality Assurance & Continuous Improvement

Professional responsibility is demonstrated through rigorous testing and continuous integration/continuous deployment (CI/CD) pipelines. Regular unit, integration, system and usability tests ensure that Janus maintains high standards of quality and reliability {REF Software testing and quality assurance guidelines (explains testing methodologies)}. Moreover, the agile development methodology and sprint planning ensure that professional standards are maintained throughout the development lifecycle (Dybå & Dingsøyr, 2008).

### Documentation

Comprehensive documentation is essential for maintaining professionalism. Janus provides detailed documentation for the CLI, along with user guides and technical documents {REF appendix}, ensuring that users and developers can understand and effectively utilise the system {REF Documentation standard in software development (provides guidelines for effective documentation)}. This clear documentation demonstrates the project’s commitment to professional clarity and accountability.

### Risk Management & Incident Response

Finally, Janus incorporates a robust risk mitigation strategy that addresses potential issues ranging from feature creep to security vulnerabilities. The use of revocable PATs, audit logging and continuous testing reflects the approach to managing professional and ethical risks; this approach safeguards the system and aligns with the professional duty to anticipate and mitigate potential threats {REF Risk management frameworks in IT (outlines best practices in risk mitigation)}.

# Project Management

## Planning & Scheduling

## Risk Management

## Tools & Techniques

# End-Project Report

## Evaluation of Objectives

# References

Anjum, N. & Alam, S., 2019. A Comparative Analysis on Widely used Web Frameworks to Choose the Requirement based Development Technology. *IARJSET,* pp. 16-24.

Chang, H., Zankl, W. & Lee, W. W., 2016. [Online]   
Available at: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection  
[Accessed 7 April 2025].

Dybå, T. & Dingsøyr, T., 2008. *Empirical studies of agile software development: A systematic review.* [Online]   
Available at: https://doi.org/10.1016/j.infsof.2008.01.006  
[Accessed 8 April 2025].

European Union, 2016. *GDPR.* [Online]   
Available at: https://www.legislation.gov.uk/eur/2016/679/contents  
[Accessed 7 April 2025].

ICO, 2025. *Transparency.* [Online]   
Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/transparency  
[Accessed 8 April 2025].

Jones, M. B., Bradley, J. & Sakimura, N., 2015. *RFC 7519.* [Online]   
Available at: https://datatracker.ietf.org/doc/html/rfc7519  
[Accessed 7 April 2025].

Kristallovich, F. & Eisfeld, H., 2020. [Online]   
Available at: https://urn.kb.se/resolve?urn=urn:nbn:se:hj:diva-50563  
[Accessed 7 April 2025].

National Instuture of Standards and Technology, 2017. *NIST Special Publication 800-63B.* [Online]   
Available at: https://pages.nist.gov/800-63-3/sp800-63b.html  
[Accessed 7 April 2025].

NIST, 2017. *Digital Identity Guidelines.* [Online]   
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf  
[Accessed 7 April 2025].

Oracle, 2025. *Transactions.* [Online]   
Available at: https://docs.oracle.com/en/database/oracle/oracle-database/19/cncpt/transactions.html  
[Accessed 7 April 2025].

OSI, 2024. *The License Review process.* [Online]   
Available at: https://opensource.org/licenses/review-process  
[Accessed 7 April 2025].

OWASP, 2025. *OWASP Cheet Sheet Series.* [Online]   
Available at: https://cheatsheetseries.owasp.org/cheatsheets/Transport\_Layer\_Security\_Cheat\_Sheet.html  
[Accessed 7 April 2025].

OWASP, 2025. *Password Storage Cheat Sheet.* [Online]   
Available at: https://cheatsheetseries.owasp.org/cheatsheets/Password\_Storage\_Cheat\_Sheet.html  
[Accessed 7 April 2025].

Parnas, D. L., 1972. *On the criteria to be used in decomposing systems into modules,* New York: Association for Computing Machinery.

Scherenberg, F. v., Hellmeier, M. & Otto, B., 2024. *Data Sovereignty in Information Systems.* [Online]   
Available at: https://doi.org/10.1007/s12525-024-00693-4  
[Accessed 8 April 2025].

Souppaya, M. & Kent, K., 2006. [Online]   
Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf  
[Accessed 7 April 2025].

Svitla, 2024. *Intellectual Property in Software Development.* [Online]   
Available at: https://svitla.com/blog/intellectual-property-software/  
[Accessed 8 April 2025].

Thomas, D. & Hunt, A., 2000. In: *The pragmatic programmer: from journeyman to master.* Boston: Addison-Wesley Longman Publishing Co., Inc..

UK Government, 2018. *Data Protection Act.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents  
[Accessed 7 April 2025].

WCAG, 2024. *Web Content Accessibility Guidelines.* [Online]   
Available at: https://www.w3.org/TR/WCAG21/  
[Accessed 7 April 2025].

# Appendices

System Architecture Diagrams

Gantt Chart

Sprint documentation

Detailed Risk Management table

User guide (Installation, minimum system requirements, usage instructions)

## User Guide

### Instillation Instructions

### Minimum System Requirements

### Usage Guide

## Project Management

Monday Board (sprints, Kanban, user stories)

Requirements, plan and sprint reviews