



UCD Michael Smurfit  
Graduate Business School

**MSc. Business Analytics**  
**MIS41170 Capstone Report**



**Managing Security & Administration of Power Platform  
Environments**

Submitted to University College Dublin in part fulfilment of the requirements of  
the degree of MSc Business Analytics

**Submitted by**

Ambarish Tirumalai (23201747)  
Priyanshu Kumar (23205386)  
Shirish Senthil Kumar (23201809)

<b>Supervisors</b>	<b>Head of School</b>
Dr. Michael MacDonnell	Professor Anthony Brabazon
Dr. Martin Perry	

## **Dedication**

This report is dedicated to all those who have inspired and supported us throughout our academic journey. To our mentors and professors, who have imparted invaluable knowledge and wisdom, guiding us towards the successful completion of this project. And to our peers, whose camaraderie and collaboration have enriched our learning experience. This work reflects your influence and a token of our deepest appreciation.

# Table of Contents

<b>TABLE OF FIGURES .....</b>	<b>5</b>
<b>PREFACE .....</b>	<b>6</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>7</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>LIST OF IMPORTANT ABBREVIATIONS .....</b>	<b>9</b>
<b>CHAPTER 1.0: INTRODUCTION .....</b>	<b>10</b>
<b>CHAPTER 2.0: LITERATURE REVIEW .....</b>	<b>11</b>
2.1 A HISTORY OF LOW-CODE PLATFORMS .....	11
2.2 POWER PLATFORMS IN THE MODERN ERA .....	12
2.3 POWER PLATFORM AND ITS COMPONENTS .....	13
2.3.1 <i>Power Platform Environments</i> .....	14
2.3.2 <i>Dataverse</i> .....	15
2.3.3 <i>Power Apps</i> .....	16
2.3.4 <i>PowerBI</i> .....	17
2.3.5 <i>Power Automate</i> .....	17
2.3.6 <i>Power Virtual Agents</i> .....	18
2.4 COMPARISON OF DIFFERENT LOW CODE APPLICATION PLATFORMS (LCAPs) .....	19
2.5 POWER PLATFORM SECURITY MEASURES .....	21
2.6 IDENTITY ACCESS MANAGEMENT (IAM) .....	22
2.6.1 <i>Authentication</i> .....	22
2.6.2 <i>Authorization</i> .....	23
2.6.3 <i>Multi-Factor Authentication</i> .....	23
2.6.4 <i>Single Sign-On</i> .....	25
2.7 SECURITY GROUPS .....	25
2.8 CURRENT SITUATION IN DATA SECURITY AND LEAKS .....	27
2.8.1 <i>Types of Data Threats</i> .....	27
2.8.2 <i>A History of Data breaches</i> .....	28
2.8.3 <i>Impact of Hacking, Poor Security, and Misconfiguration</i> .....	30
2.9 OVERVIEW OF ROLE-BASED ACCESS CONTROL (RBAC) IN HEALTHCARE .....	31
<b>CHAPTER 3.0: METHODOLOGY AND APPROACH .....</b>	<b>32</b>
3.1 SYNTHETIC RELATIONAL DATABASES AND SIMULATED DATA .....	33
3.2 SIMULATED SHARING SCENARIOS AND SYNTHETIC ACTIVITY LOGS .....	33
3.3 DATA GOVERNANCE AND FINANCIAL DATA .....	33
3.4 CHOSEN STRATEGY .....	34
3.5 ADVANTAGES OF METHODOLOGY .....	34
3.6 LIMITATIONS OF THE METHODOLOGY .....	35
<b>CHAPTER 4.0: OBJECTIVES AND DELIVERABLES .....</b>	<b>35</b>
4.1 ENHANCING SECURITY COMPLIANCE .....	36

4.2 RISK REDUCTION .....	36
4.3 MODELLING POTENTIAL DATA BREACHES WITH PRACTICAL CASE STUDY IN HEALTHCARE INDUSTRY .....	37
4.4 COMPREHENSIVE DOCUMENTATION AND TRAINING.....	37
4.5 SUCCESS METRICS FOR CASE STUDY AND CAPSTONE .....	38
<b>CHAPTER 5.0: DATA SECURITY CASE STUDY: A HEALTHCARE APP .....</b>	<b>39</b>
5.1 POWER APPS.....	39
5.2 DATAVERSE .....	40
5.3 APP USER INTERFACE.....	41
5.4 ROLES IMPLEMENTED IN THE CASE STUDY .....	42
5.5 HOW IS RBAC IMPLEMENTED? .....	43
5.6 MULTI FACTOR AUTHENTICATION .....	44
5.7 SINGLE SIGN ON.....	45
5.8 IMPLEMENTATION OF SECURITY GROUPS.....	45
5.8.1 Pharmacist – Hospital Employee .....	46
5.8.2 Junior System Administrator – IT Systems .....	46
5.8.3 Senior System Administrator – IT Systems .....	47
<b>CHAPTER 6.0: WORKING OF THE APP .....</b>	<b>47</b>
6.1 DATA PROTECTION FEATURE USING RBAC .....	55
<b>CHAPTER 7.0: ARCHITECTURE OF THE APP .....</b>	<b>59</b>
7.1 DATA LOSS PREVENTION POLICIES .....	60
7.2 IMPLEMENTATION OF DATA LOSS PREVENTION (DLP) IN OUR PROJECT .....	61
<b>CHAPTER 8.0: RESULTS AND CONCLUSION.....</b>	<b>63</b>
8.1 RESULTS.....	63
8.2 CONCLUSION .....	64
<b>CHAPTER 9.0: FUTURE WORK AND SCOPE.....</b>	<b>64</b>
<b>CHAPTER 10.0: REFERENCES .....</b>	<b>65</b>
<b>APPENDIX.....</b>	<b>75</b>
Code for Login button.....	75

# Table of Figures

Figure 1. Products of Power Platform (Wang, 2023) .....	13
Figure 2. Power Platform Capabilities (Wang, 2023) .....	14
Figure 3: Top 20 data breaches by company .....	29
Figure 4: Most common data breach methods .....	30
Figure 5: Login page of the app .....	41
Figure 6: Multi-Factor Authentication Setup (Justinha, 2023) .....	44
Figure 7: Single Sign-on setup (Shukla & Jain, 2016) .....	45
Figure 8: Security Roles in Healthcare Scenario .....	46
Figure 9: Pharmacist Role Permission Access Controls .....	46
Figure 10: Junior System Administrator Role and Permission Controls .....	47
Figure 11: Senior System Administrator and Permission Access Controls .....	47
Figure 12: Doctor's Page .....	48
Figure 13: Doctor's Patient Details Page .....	49
Figure 14: Doctors - Uploading Prescriptions .....	50
Figure 15: Pharmacist's page.....	51
Figure 16: Pharmacists - Inventory Page .....	52
Figure 17: Sample Inventory Table .....	52
Figure 18: Receptionist's Screen.....	53
Figure 19: Receptionist - Patient Details screen .....	54
Figure 20: Receptionist - Sample Patient Details .....	54
Figure 21: Receptionist - Viewing Appointment Details .....	55
Figure 22: Unsuccessful Login Error Page .....	56
Figure 23: IncorrectLogins Table .....	57
Figure 24: Email Trigger Power Automate Flow .....	57
Figure 25: Row Modification Details in Power Automate Flow.....	58
Figure 26: Email Details in Power Automate Flow .....	58
Figure 27: Architecture of the app .....	59
Figure 28: Data Loss Prevention Policy - Allowed Connectors .....	61

# Preface

The rise of low-code platforms like Microsoft's Power Platform is reshaping how enterprises develop and deploy software. These tools offer immense flexibility and speed, allowing businesses to create custom applications quickly. However, with these advantages come significant security and governance challenges that, if not addressed, can lead to serious vulnerabilities.

This report was developed to explore these challenges and provide a practical framework for managing Power Platform environments securely. It begins with an introduction to the platform's core components and their role in digital transformation. It then delves into the specific risks and governance issues that organizations face when using Power Platform.

The report offers a structured methodology for implementing key security measures, including Identity Access Management (IAM) and Role-Based Access Control (RBAC). A real-world case study illustrates these strategies in action, providing practical insights and lessons learned.

Finally, the report concludes with actionable recommendations to help organizations enhance their security and governance of Power Platform environments.

This report is intended for IT professionals and business leaders seeking to secure their Power Platform deployments while maximizing their potential.

Ambarish Tirumalai (23201747)  
Priyanshu Kumar (23205386)  
Shirish Senthil Kumar (23201809)

*Dublin, Ireland*

*August 2024*

# Acknowledgements

We would like to express our deepest gratitude to all those who have supported and guided us throughout the completion of this capstone project, "Managing Security & Administration of Power Platform Environments."

First and foremost, we are immensely grateful to our supervisor, Dr. Michael MacDonnell, for his invaluable guidance, insightful feedback, and unwavering support during the course of this project. His expertise and encouragement were instrumental in shaping our research and helping us overcome challenges.

We extend our sincere thanks to Kathleen Griffin from Microsoft Ireland, for her expert insights and assistance with navigating the complexities of Power Platform. Her contributions were vital in deepening our understanding of the platform and its security and governance aspects.

Our appreciation also goes to our academic institution, particularly the MSc. Business Analytics program, for providing us with the knowledge and resources necessary to undertake this project. The skills and insights gained throughout this program have been pivotal in the successful completion of this report.

We would also like to acknowledge the contributions of our peers and colleagues who provided constructive criticism and helpful suggestions during the various stages of our research. Their input has been invaluable in refining our work.

Finally, we express our heartfelt appreciation to our families and friends for their constant encouragement and support, without which this project would not have been possible.

# Executive Summary

The adoption of low-code platforms like Microsoft's Power Platform is revolutionizing how organizations develop and deploy business applications. While these platforms offer unparalleled speed and flexibility, they also introduce significant security and governance challenges. This report, "Managing Security & Administration of Power Platform Environments," provides a detailed analysis of these challenges and outlines strategic solutions.

## Background and Scope

Power Platform enables rapid development of custom applications, making it an essential tool in modern enterprises. However, as its use expands, so do the risks associated with data security, unauthorized access, and compliance. This report addresses these issues, offering a comprehensive governance framework tailored to Power Platform environments.

## Key Findings

The report identifies critical vulnerabilities in Power Platform environments, including risks related to data breaches and inadequate access controls. It also highlights the importance of implementing robust security measures such as Identity Access Management (IAM), Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA) to mitigate these risks.

## Case Study and Recommendations

A case study included in the report demonstrates the successful implementation of security and governance strategies in a real-world organization. Based on this analysis, the report offers actionable recommendations for enhancing security and governance, emphasizing the need for continuous monitoring and proactive risk management.

The report concludes that while Power Platform provides significant advantages in terms of agility and efficiency, these benefits can only be fully realized with a strong security and governance framework. Organizations that adopt the strategies outlined in this report will be better positioned to protect their data, ensure compliance, and maximize the value of their Power Platform investments.



# List of important abbreviations

1. LCP: Low Code Platform
2. DBIR: Data Breach Investigations Report
3. DLP: Data Loss Prevention
4. IAM: Identity Access Management
5. MFA: Multi-Factor Authentication
6. RBAC: Role-Based Access Control
7. SSO: Single Sign-On
8. OIDC: OpenID Connect
9. SAML: Security Assertion Markup Language
10. PCI DSS: Payment Card Security Data Security Standard
11. HIPAA: Health Insurance Portability and Accountability Act - 1996
12. GDPR: General Data Protection Regulation
13. AAD: Azure Active Directory
14. API: Application Programming Interface
15. AWS: Amazon Web Services

# Chapter 1.0: Introduction

The growing adoption of low-code platforms, such as Microsoft's Power Platform, has revolutionized how enterprises build and deploy business applications. The Power Platform enables users to create custom applications, automate workflows, and analyze data with minimal coding knowledge. However, with the adoption of these platforms at an enterprise level and their scalability necessitate robust governance and administration frameworks to manage and mitigate risks effectively.

As per an analysis performed by (Verizon, 2024), there has been a significant increase in attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach in data platforms when compared to previous years. This underscores the importance of proper safeguards against any attacks or inadvertent data breaches. The main vector for those initial entry points for data breaches was web applications (Verizon, 2024). Therefore, power platforms, being a set of web applications, are sometimes considered to be a point of vulnerability as far as data breaches are concerned.

Keeping the data of the people using the platform safe (and also those of the people whose data is in the system) has to be the first priority of the governance, security, and administrative frameworks on the power platform. Cyber threats to the data, inadvertent data issues, and others are problems that can happen without anyone's knowledge. Cyber threats, in particular, remain at the forefront of global security challenges, as opportunistic and resilient adversaries exploit vulnerabilities through sophisticated tactics (Flashpoint, 2024). Therefore, it is important to consider any and all kinds of threats, not just when using the power platforms but also when monitoring and governing their usage by the various stakeholders. Consequently, a portion of the organisation's resources should be dedicated to protecting itself from security incidents; preventive measures include maintaining regular backups, keeping software up to date, and employee education in order to reduce miscellaneous errors (Sarabi, et al., 2016).

Our project, "Managing Governance and Administration of Power Platform Environments," aims to address the risks associated with scaling Power Platform solutions at an enterprise level. These risks include security compliance issues, data leakage, apps without valid owners, and apps that

are shared too broadly within the organization. Without proper governance, these risks can lead to significant operational inefficiencies and potential security breaches.

## **Chapter 2.0: Literature Review**

### **2.1 A history of Low-code platforms**

In recent years, the digital landscape has been transformed into a landscape where the development is done by anybody who has an idea about a particular idea. It is widely known that the lack of professional software developers is a major obstacle for many companies in successfully dealing with digital transformation. Moreover, there is the perennial problem that software development projects often suffer from poor efficiency or fail altogether (Bock & Frank, 2021).

This is the talking point for most Low Code Platforms (LCP) by vendors and market research firms. According to Vincent et al. (2019), “enterprise low-code application platforms deliver high productivity and multifunction capabilities across central, departmental and citizen IT functions”. These platforms empower users, including those with minimal coding experience, to create and deploy applications effectively, addressing the shortage of skilled developers and enhancing project success rates.

An interesting fact of all products considered “low code” is that they have existed in one form or another, even before the term “low code” was officially coined. These products have often been the primary offerings of companies for years or decades. This can be substantiated with different “low code” examples such as Platform-as-a-Service (PaaS) and Business Process Management (BPM) tools (Bock & Frank, 2021).

Therefore, it can be said that though LCPs have existed for a while, it is still playing a big role in transforming the business environment for many companies. According to Oluwaseyi (2024), a couple of factors play a role here: firstly, these paradigms enable rapid prototyping and deployment, reducing time-to-market for applications. And secondly, they empower non-technical users, such as business analysts and domain experts, to actively participate in the development process, leading to better alignment between IT and business goals.

As the business landscape continues to evolve, so too do the tools and platforms that support it. One such advancement is the emergence and adoption of power platforms. In the modern era, power platforms are paving the way for improved development and automation, offering a suite of tools to enhance productivity and collaboration.

## **2.2 Power Platforms in the Modern Era**

The emergence of the Microsoft Power Platform represents a pivotal moment in the realm of modernization and digital transformation. With its ability to significantly reduce the time, cost, and prerequisites associated with such initiatives, the platform has garnered widespread attention from organizations seeking to innovate and adapt in today's fast-paced market (Standefer & Yack, 2023).

Notably, the Power Platform has achieved remarkable adoption worldwide, serving as the cornerstone of digital transformation for organizations in the modern era. In fact, a staggering 97% of Fortune 500 companies have embraced its capabilities, leveraging them to streamline operations, enhance productivity, and foster innovation (Dataworks, n.d.)

As explained by Standefer and Yack (2023), a key aspect of the Power Platform's appeal lies in its ability to empower both citizen developers and professional developers alike. Citizen developers, possessing domain expertise but limited technical skills, can now actively participate in the modernization process. By leveraging their specialized knowledge, they can create tailored solutions while reducing dependence on IT teams. Conversely, professional developers can expedite the delivery of complex solutions, optimizing resource allocation and enhancing project outcomes.

Beyond its widespread adoption in the corporate world, power platforms have permeated diverse sectors, from healthcare to fintech and manufacturing. Their versatility and adaptability make them a preferred choice for organizations seeking agile solutions to complex challenges.

## 2.3 Power Platform and its Components

Power Platform is a suite of Microsoft tools designed to empower users to build custom applications, automate workflows, analyze data, and create virtual agents without extensive coding knowledge. It comprises four main components: Power BI, Power Apps, Power Automate, and Power Virtual Agents as shown in Figure 1. Power BI allows users to visualize data and share insights across their organization. Power Apps enables the creation of custom applications to solve business challenges. Power Automate (formerly Microsoft Flow) facilitates the automation of repetitive tasks and workflows. Power Virtual Agents allows the creation of intelligent chatbots to engage with customers and employees (Wang, 2023).

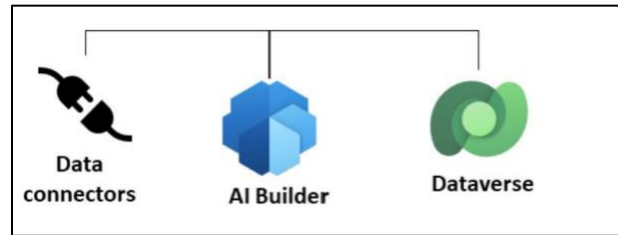


*Figure 1. Products of Power Platform (Wang, 2023)*

Scalability is a key feature of Power Platform, allowing solutions to grow with the organization's needs. (Palmer, 2020). It empowers individuals with domain knowledge to develop and deploy robust solutions without deep technical expertise, thanks to its low-code/no-code approach. This democratization of app development means that business experts can create, iterate, and implement solutions quickly, driving innovation and efficiency while reducing dependency on IT departments (Binzer & Winkler, 2022). By enabling domain experts to directly produce outputs, Power Platform accelerates time-to-value and fosters a more agile and responsive business environment.

Additionally, the Power Platform includes robust features such as AI Builder, which adds artificial intelligence capabilities like image recognition, text analysis, and predictive modeling to apps without requiring extensive coding. Dataverse, formerly known as the Common Data Service, provides a secure and scalable data storage solution that integrates seamlessly with Power Platform applications, facilitating unified data management and accessibility. The platform also offers an extensive array of data connectors, enabling users to easily connect to a wide variety of data

sources, from traditional databases and cloud-based services to on-premises systems, enhancing its versatility and allowing for comprehensive data integration and flow across diverse environments (Wang, 2023). These technologies are shown in Figure 2 with their icons.



*Figure 2. Power Platform Capabilities (Wang, 2023)*

### **2.3.1 Power Platform Environments**

Power Platform environments are specialized spaces designed to store, manage, and share an organization's business data, applications, chatbots, and workflows. These environments serve as containers to segregate applications based on different roles, security requirements, or target audiences, ensuring each application has the appropriate resources and security settings tailored to its specific needs. (Herrera, 2022)

Organizations can create multiple environments to support various stages of application development, such as development, testing, and production. This separation helps maintain a clear distinction between phases of the app lifecycle, ensuring stability and reducing risks associated with changes and updates. Environments can also be tailored for different departments or projects, providing dedicated spaces for each to manage their applications without interference, which is especially useful for larger organizations with multiple teams (Wadiwala & India, 2019).

Power Platform environments include advanced security controls to ensure data integrity and confidentiality. Each environment operates with its own security boundaries, allowing for precise management of access and permissions through role-based access control (RBAC). This granular permission model prevents unauthorized access and modifications, ensuring only authorized personnel can interact with sensitive data (Ajish, 2024).

Key security features include data loss prevention (DLP) policies that restrict data movement between business and non-business connectors to prevent leaks (Wadiwala & India, 2019). Environments support encryption both at rest and in transit, using industry-standard protocols to protect data. Comprehensive auditing and monitoring capabilities provide visibility into data access and changes, while integration with Azure Active Directory (AAD) enables single sign-on (SSO) and multi-factor authentication (MFA) for enhanced security (Sufi, 2023).

### **2.3.2 Dataverse**

Dataverse is a comprehensive data platform within Power Platform designed to securely store, manage, and utilize business data across various applications. The data in Dataverse is organized into tables, consisting of rows and columns, where each column stores a specific type of information like names, ages, or salaries. (Evans & Petersson, 2023). While standard tables are available to cover common scenarios, Dataverse also supports the creation of custom tables that can be populated using Power Query (Reza, 2023). This flexibility allows app makers to build sophisticated applications in Power Apps that leverage the stored data efficiently.

Dataverse simplifies the complex and often costly process of building a data infrastructure to derive business insights. It offers an easy-to-use, scalable, and compliant SaaS data service that supports any type of data and application. With minimal coding requirements, Dataverse can be utilized by both knowledge workers and professional developers (Wang, 2023). Built on Azure, it guarantees global availability, robust compliance, and advanced security. The platform integrates all major data technologies—relational, non-relational, file, image, search, and data lake—providing a versatile solution for diverse data needs. (Gannon, et al., 2014)

Security and administration in Dataverse are robust, featuring advanced measures to protect data integrity and confidentiality. Role-based access control (RBAC) allows precise management of permissions, ensuring only authorized users can access or modify data. Data is encrypted both at rest and in transit, protecting it from unauthorized access. (Herrera, 2022). Comprehensive auditing and monitoring tools provide detailed logs of data interactions, aiding compliance and security oversight. Additionally, Dataverse's visual designers streamline the creation and

management of tables, relationships, business rules, forms, and workflows, ensuring easy administration and robust data governance.

### **2.3.3 Power Apps**

Power Apps, a pivotal element of the Power Platform, simplifies application development with its modern, agile framework and user-friendly “what you see is what you get” (WYSIWYG) environment. This allows users to create high-quality products swiftly, bypassing the lengthy cycles of traditional development methods (Leung & Leung, 2021). Its versatility extends beyond corporate confines, benefiting organizations in Ireland, including public institutions and SMEs, fostering efficiency and innovation. Particularly advantageous in low-code development projects, Power Apps enables companies to harness their employees' domain expertise to construct applications without extensive coding expertise (Palmer, 2020)

With a strong emphasis on data security and compliance, Power Apps aligns with regulatory standards such as the General Data Protection Regulation (GDPR). Through robust security measures such as role-based access control (RBAC), encryption, and data masking, it safeguards sensitive information from unauthorized access or disclosure. The platform's adherence to compliance certifications like GDPR, ISO 27001, and SOC underscores its commitment to meeting stringent security and privacy standards. (Miyake, et al., 2023)

Administering Power Apps within organizations entails managing user access, permissions, and data governance to ensure compliance with regulatory requirements. Integration with Microsoft Entra ID (formerly Azure Active Directory) simplifies centralized identity management and authentication, while audit logs offer transparency into data interactions for compliance monitoring (Wilhelms, 2024). Additionally, Power Apps supports data residency and sovereignty requirements, allowing organizations to store data in specific regions to comply with local regulations. (Di Ruscio, et al., 2022)Power Apps provides a robust and secure platform for application development, empowering organizations to innovate and drive business growth while maintaining compliance with regulatory standards.



### **2.3.4 PowerBI**

Power BI, an integral component of the Power Platform, revolutionizes data analysis and visualization with its intuitive interface and powerful analytics capabilities. It empowers users to transform raw data into actionable insights swiftly, enabling informed decision-making across organizations. With its user-friendly features and comprehensive toolset, Power BI caters to diverse user needs, from individual analysts to large enterprises, driving efficiency and enhancing productivity. (Gautam & Kumar, 2023)

In low-code development projects, Power BI proves invaluable by allowing users to create data visualizations and reports without extensive technical expertise. This democratization of data analysis enables organizations to leverage their domain knowledge effectively, extracting meaningful insights from their data to drive business growth. (Heine, et al., 2023)

Moreover, Power BI offers additional security features such as row-level security, data loss prevention (DLP) policies, and secure data gateways. These features further enhance data protection and help organizations prevent unauthorized access and data leaks. In terms of data recovery, Power BI provides built-in capabilities for data restoration, including version history and backups, ensuring business continuity and data resilience.

### **2.3.5 Power Automate**

Microsoft's Power Automate is a versatile tool within the Power Platform that aims to streamline repetitive and time-consuming tasks. It provides a user-friendly, low-code environment where individuals can create workflows that integrate various services and applications, thereby enhancing productivity and operational efficiency (Microsoft, 2022). The platform supports different types of automated processes, including cloud-based flows and robotic process automation (RPA), and incorporates artificial intelligence (AI) to offer intelligent automation solutions. Power Automate's deep integration with the Microsoft 365 ecosystem and other Power Platform tools makes it a comprehensive solution for automating business processes across an organization.

The cloud flows in Power Automate allow users to create workflows using a drag-and-drop interface, seamlessly integrating with services like Microsoft Teams, SharePoint, and Dynamics 365 (Microsoft, 2022). The platform's RPA capabilities enable the automation of desktop processes, particularly useful for tasks involving legacy systems. AI Builder further enhances these workflows by integrating machine learning models, enabling the automation of tasks such as document processing and sentiment analysis (Microsoft, 2022). Additionally, the Co-pilot feature leverages AI to assist users in creating and managing workflows, suggesting improvements, and troubleshooting issues to optimize automation processes (Microsoft, 2024).

Power Automate can significantly streamline various business processes. For instance, it can automate document processing by extracting data from forms and reducing manual data entry. In customer service, it can integrate with CRM systems to automate follow-up emails and update customer records, enhancing response times and customer satisfaction. Furthermore, its governance features help ensure that workflows adhere to regulatory requirements, maintaining compliance and improving overall governance within the organization.

### **2.3.6 Power Virtual Agents**

Microsoft's Power Virtual Agents enable businesses to create sophisticated chatbots without requiring coding expertise. These chatbots can interact with customers and employees, providing support, answering questions, and automating service processes. The intuitive interface allows users to design conversation flows and integrate them with various services and databases, making it easy to deploy effective virtual agents (Microsoft, 2024).

It also offers a no-code bot-building experience, allowing users to design and deploy chatbots using a graphical interface. These bots can seamlessly integrate with other Power Platform tools, such as Power Automate and Power Apps, to facilitate advanced automation scenarios. The platform's AI capabilities, including natural language processing, ensure that the bots can understand and respond to user queries effectively. Furthermore, Power Virtual Agents can be customized and extended by integrating with external APIs and services, providing businesses with the flexibility to tailor the bots to their specific needs (Microsoft, 2024).

It can be leveraged to enhance customer support by handling common inquiries, providing product information, and guiding users through troubleshooting steps, freeing up human agents for more complex issues. Internally, these bots can assist employees with IT support, HR queries, and accessing company resources, improving efficiency and response times. In the e-commerce sector, Power Virtual Agents can aid customers with product searches, order tracking, and personalized recommendations, enhancing the overall customer experience (Microsoft, 2024).

## 2.4 Comparison of different Low Code Application Platforms (LCAPs)

Gartner defines Low Code Application Platforms (LCAPs) as application platforms that are used to rapidly develop and run custom applications by abstracting and minimizing the use of programming languages (Matvitskyy, et al., 2023). These platforms must be supported by various features, both in the security realm and otherwise, for them to be effective in app creation. In view of this, let us compare the various security features of the Microsoft Power Platforms with other LCAP providers. To do so, let us consider a few factors on which the security of LCAPs is based.

### 1. Authentication and Authorization

- a. Power Platforms: Uses Microsoft Entra ID (Formerly Azure Active Directory) for authentication, employing industry-standard OAuth 2.0 for secure API access. It offers robust Role Based Access Control (RBAC) to manage permissions (Microsoft, 2022)
- b. Other platforms: LCAPs such as Amazon Honeycode uses AWS Identity and access management for secure user authentication and access control, with fine-grained permission settings (Barr, 2020). Salesforce Lightning and Outsystems use features like Single Sign On (SSO) or Multi-Factor Authentication (MFA) (Codemotion, 2022)

### 2. Data protection and privacy

- a. Power Platforms: Data is encrypted both at rest and in transit, due to Microsoft Azure's security infrastructure. It supports Data Loss Prevention (DLP) policies to control data sharing and prevent leaks (Microsoft, 2022).
- b. Other platforms: Standard data encryption and tools like Amazon Macie for data privacy and security compliance in Amazon Honeycode, including encryption and monitoring for data at rest and in transit (AWS risk and compliance whitepaper pdf).

Salesforce Lightning has an additional feature called Salesforce Shield protecting the data (Codemotion, 2022).

### **3. Compliance and Certifications**

- a. Power Platforms: Complies with multiple certifications, including GDPR, HIPAA, ISO 27001 and SOC 2. It also provides tools for auditing and managing access to sensitive data (Microsoft, 2022).
- b. Other platforms: Amazon Honeycode inherits a wide range of compliance certifications, such as PCI DSS, HIPAA and GDPR, offering robust audit and compliance tools. Salesforce Lightning complies with the certifications of Power platforms as well, with OutSystems complying with ISO 22301 as well (Amazon, 2024).

### **4. Threat detection and response**

- a. Power Platform: Integrates with Microsoft Defender for Cloud apps for advanced threat detection, providing alerts and automated responses to potential security incidents. Can leverage the automated flows of Power Automate as well to detect threats and send out alerts (Microsoft, 2022).
- b. Other Platforms: Honeycode uses AWS security tools like Amazon GuardDuty for continuous threat detection, monitoring unusual activity across AWS accounts (Barr, 2020). OutSystems and Mendix provide these as well.

### **5. API and Integration Security**

- c. Power Platforms: Secure APIs with OAuth 2.0, extensive logging and auditing capabilities, and also offers secure integration with other Microsoft services and third-party apps (Microsoft, 2022). However, it is restricted to the common layer of Dataverse (Matvitskyy, et al., 2023).
- d. Other Platforms: Honeycode leverages AWS's security features for secure API management, including access control and detailed logging (Amazon, 2024). Salesforce Lightning provides API management through OAuth, SAML and API access controls, whereas OutSystems ensures API security through strong authentication, encryption and access controls.

## 2.5 Power Platform Security Measures

Power Platform integrates advanced security protocols to protect data and applications, ensuring user information is safeguarded, data integrity is maintained, and potential threats are mitigated. Addressing access control, data classification, secure data transfer, and regulatory compliance, the platform's robust security framework defends against unauthorized access and cyber threats. Here are specific security features that enhance Power Platform's security capabilities.

1. **Conditional Access Policies:** These policies are used to enforce specific conditions under which users can access resources. For example, access can be restricted based on the user's location, device compliance, or risk level, adding an extra layer of security. Identity and Access Management (IAM) is also employed to manage user identities and control access to resources, ensuring that only authorized users can access sensitive data and applications. (Shukla & Jain, 2024)
2. **Data Classification and Sensitivity Labels:** Power Platform allows for the classification of data based on sensitivity. Sensitivity labels can be applied to data to enforce encryption, restrict sharing, and ensure that sensitive information is handled appropriately. Additionally, Data Loss Prevention (DLP) policies can be implemented to prevent the inadvertent sharing of sensitive information, ensuring that data is used in compliance with organizational policies and regulations (Wadiwala & India, 2019).
3. **Secure Data and Web Gateways:** These gateways enable secure data transfer between on-premises data sources and Power Platform applications. This ensures that data remains protected while being integrated from various sources. (Deckler, et al., 2022)
4. **IP Address Filtering and Firewalls:** Administrators can configure IP address filtering to restrict access to Power Platform environments only from specified IP addresses, reducing the risk of unauthorized access. Firewalls can also be employed to provide an additional layer of security by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. (Ullrich, et al., 2016)
5. **Tenant Isolation:** Power Platform supports tenant isolation to ensure that data and applications are securely separated between different tenants, preventing cross-tenant data breaches (Ochei, et al., 2023).

6. **Application Security:** Power Apps and other components of Power Platform support app-specific security configurations, including app-level permissions and the ability to implement custom security logic using Microsoft Dataverse. Role-Based Access Control (RBAC) is also utilized to ensure that users have access only to the data and functions necessary for their roles, enhancing security by limiting exposure to sensitive information and critical functions based on user roles. (Ajish, 2024)
7. **Secure APIs:** Power Platform uses secure APIs with OAuth 2.0 authentication to ensure that data interactions between applications and services are protected (Ferry, et al., 2015)
8. **Advanced Threat Protection:** Integration with Microsoft Defender for Cloud Apps provides advanced threat detection and response capabilities, helping to identify and mitigate potential security threats (Rising, 2023).
9. **Data Masking:** Data masking techniques can be applied to protect sensitive data within applications, ensuring that sensitive information is obscured from unauthorized users (L'Esteve, 2022).
10. **Compliance Certifications:** Power Platform adheres to various compliance standards and certifications, such as GDPR, ISO 27001, and SOC, ensuring that the platform meets rigorous security and privacy requirements. (Miyake, et al., 2023)

## **2.6 Identity Access Management (IAM)**

Effective Identity and Access Management (IAM) is vital for maintaining the security and integrity of data within the Power Platform ecosystem. IAM encompasses both authentication and authorization processes to ensure that only verified and authorized users can access sensitive information and perform specific actions within the system.

### **2.6.1 Authentication**

Authentication is the process of confirming the identification of a user or system to ensure that they are who they claim to be. In the context of power platforms, authentication is crucial as it establishes a basic level of confidence in user identity, ensuring secure access to sensitive data and applications. Common authentication techniques include passwords, biometrics (such as fingerprints or face recognition), one-time pins (OTPs), and security code-generating

authentication apps. Multi-factor authentication (MFA) is extensively used, requiring two or more verification methods to provide greater protection than a single password. (Okta, 2023; OneLogin, n.d.) This method is critical for protecting access to systems and data, ensuring that only authorised users can enter secure environments. A key example in this domain is Microsoft Entra ID, which provides robust identity, and seamless single sign-on (SSO) capabilities access management solutions to enhance security and streamline user authentication processes (Chik, 2024).

### **2.6.2 Authorization**

Authorization, on the contrary, is the process of determining what an authenticated user can do within a system. In the context of power platforms, authorization specifies the rights and access levels granted to the user, delineating the resources and functions they can access. For instance, within a corporate power platform, a manager may have elevated access to sensitive data and administrative capabilities compared to a regular employee. Role-based access control (RBAC) assigns permissions based on user roles, while rule-based access control grants or denies access through specified rules and policies (Auth0, n.d.; Mehta, n.d.). Authorization ensures that users can only interact with data and systems in ways that are consistent with their roles and responsibilities.

Microsoft Entra ID plays a pivotal role in managing these authorization processes. It provides a comprehensive identity and access management solution that supports RBAC and integrates seamlessly with power platforms to enforce secure and efficient access controls. Entra ID offers advanced features such as conditional access policies, identity protection, which help organizations manage user permissions and protect sensitive information. By leveraging Microsoft Entra ID, businesses can ensure that their authorization protocols are robust, scalable, and aligned with best practices for security and compliance (Chik, 2024).

### **2.6.3 Multi-Factor Authentication**

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of verification before accessing resources. Over the years, MFA has evolved significantly. Initially, systems relied solely on passwords, which were often vulnerable to attacks like phishing and brute force (Ometov, et al., 2018). MFA was introduced to address these

weaknesses by requiring additional verification methods such as phone calls, text messages, mobile app notifications, one-time passwords (OTP), emails, and even biometric verification (Hossain, et al., 2024). This approach significantly enhances security by making it much harder for unauthorized users to gain access.

Implementing MFA in Microsoft Entra ID, formerly known as Azure Active Directory, can be done through various user-friendly methods designed to enhance security without compromising convenience. One of the key strategies is using Conditional Access Policies. These policies allow administrators to define specific conditions—like user location, device compliance, and application access—that trigger MFA (Kasahara & Shimayoshi, 2022). This ensures that additional security measures are applied only when necessary, striking a balance between protection and ease of use. By tailoring the conditions for MFA, organizations can maintain high security standards while minimizing disruptions for users.

Organizations require a Microsoft Entra ID tenant, to add users that they would like to enable MFA, which is usually all the employees (Justinha, 2023). The rationale behind this inclusive approach is that high-profile individuals, such as executives, are often targeted more frequently by attackers due to their access to sensitive information and key decision-making power (Sherstobitoff, 2008). Further, it is configured to the app of choice that needs Multi-Factor Authentication and enabled. The authentication needs to be thoroughly tested before deployment to the organization, to avoid data breaches and continue operational efficiency.

Despite its benefits, implementing Multi-Factor Authentication (MFA) in Azure Active Directory (AD) presents several challenges. One significant hurdle is user resistance, as many users may perceive MFA as inconvenient or may lack awareness of its importance, leading to reluctance in adoption (Pureti, 2020). Additionally, the cost can be a barrier, especially when organizations opt for hardware tokens or premium authentication methods, which can incur significant expenses (Liou & Bhashyam, 2010). Furthermore, the complexity of configuring and managing MFA policies requires careful planning and expertise to ensure effective implementation, making it a challenging task for IT departments (Liou & Bhashyam, 2010).

To maximize the effectiveness of MFA in Azure AD, organizations should consider several best practices. First, user education is crucial; educating users on the importance of MFA and providing



clear instructions on setting up and using MFA methods can significantly enhance adoption and compliance (Reno, 2013). Implementing MFA in phases, starting with high-risk users and gradually extending to the entire organization, can help manage the transition smoothly and address any issues incrementally (Proctor, et al., 2017). Additionally, regularly reviewing and updating MFA policies is essential to adapt to emerging threats and changing organizational needs, ensuring that the security measures remain robust and effective (Roopesh, 2024).

#### **2.6.4 Single Sign-On**

Single Sign-On (SSO) is a user authentication process that allows a person to access multiple applications with one set of login credentials. It aims to simplify user experience and enhance security by reducing the number of passwords users need to remember and manage (De Clerq, 2002).

The concept of SSO dates back to the early days of enterprise computing when organizations started to adopt multiple IT systems and applications. Initially, each system required separate login credentials, leading to "password fatigue" among users and increasing the risk of security breaches due to weak or reused passwords (Chitalia, et al., 2013). SSO has evolved with advancements in technology and increasing security demands. Modern SSO solutions incorporate advanced authentication methods, such as multi-factor authentication (MFA), to further enhance security (Pandey & Nisha, 2017).

SSO can be configured in two methodologies, namely Security Assertion Markup Language (SAML) and OpenID Connect (OIDC). SAML is an XML-based standard commonly used for enterprise and legacy applications, while OpenID Connect is a modern authentication protocol built on OAuth 2.0, ideal for web and mobile applications (Mainka, et al., 2017).

### **2.7 Security Groups**

Security groups in the Power Platform are crucial for managing user access and permissions within an organization. Within the RBAC framework, security groups allow administrators to assign roles efficiently based on groups rather than individual user settings (Thakare, et al., 2020). For example, an Administrative Security Group might be created to grant full control over Power Platform environments, including the ability to create, modify, and delete resources. This group ensures that

only users who need administrative privileges are granted such access, minimizing the risk of unauthorized changes (Leung & Leung, 2021).

On the other hand, an End-User Security Group can be established to provide basic access to applications without the ability to make any alterations. This setup is particularly useful for users who only need to interact with the applications as consumers, ensuring they have the necessary access without the risk of accidental modifications (Tverhasselt, 2024). By leveraging security groups in this way, organizations can ensure that each user has the appropriate permissions for their role, enhancing both security and efficiency.

Implementation of security groups with the Power Platform's RBAC framework is managed through the Power Platform Admin Center. This centralized management allows for efficient handling of user access, where adding or removing users from security roles in the Power Platform Admin Center dynamically adjusts their permissions across the entire platform (Herrera, 2022).

Additionally, security groups can be used to control access at the environment level within the Power Platform. For instance, members of a designated Production Admins group might be the only users granted access to the production environment. This granular control over environment access enhances security by ensuring that users can only interact with the data and resources necessary for their roles, maintaining a secure and organized operational environment (Herrera, 2022).

### **Benefits of Using Security Groups**

The use of security groups within the Power Platform offers several key benefits. It simplifies administration by allowing for easy management of user permissions at large scale, as changes to group members automatically reflect across all linked services. Additionally, security groups ensure consistent permissions application, reducing the risk of errors or unauthorized access, and helping organizations enforce the principle of least privilege. This streamlined and scalable approach to access management significantly enhances the organization's security framework (Herrera, 2022).

## 2.8 Current Situation in Data Security and Leaks

The current landscape of data breaches illustrates a significant rise in incidents affecting various industries. Notably, data breaches have compromised sensitive information, including social security numbers, bank account information, and medical data, leading to substantial repercussions for the affected organizations and individuals (Juma'h & Alnsour, 2019). Major companies such as Equifax, Anthem, eBay, JPMorgan Chase, Home Depot, Yahoo, and Target have all experienced substantial breaches, underscoring the pervasive nature of this issue (Juma'h & Alnsour, 2019).

Recent data from the Verizon 2024 Data Breach Investigations Report (DBIR) highlights that the number of breaches continues to grow, with the majority of these incidents involving external actors exploiting vulnerabilities within organizational systems. The report indicates that the primary methods of attack include phishing, use of stolen credentials, and exploitation of vulnerabilities, leading to unauthorized access and data exfiltration (Verizon, 2024).

Similarly, the Flashpoint 2024 Global Threat Intelligence Report emphasizes a notable increase in data breach activities. In 2023, Flashpoint recorded 6,077 publicly reported breaches, a 34.5% increase from the previous year. These breaches resulted in the exposure of over 17 billion personal records, with the United States accounting for more than 60% of these incidents (Flashpoint, 2024). The report attributes over 70% of these breaches to unauthorized access, further highlighting the critical need for robust security measures and effective threat intelligence (Flashpoint, 2024).

### 2.8.1 Types of Data Threats

Data threats come in various forms, each with its own unique risks and requiring specific strategies to address them. Hacking, which involves unauthorized access to data systems by exploiting vulnerabilities or weak security measures, is a significant threat. Malware, such as viruses, worms, and spyware, is designed to infiltrate and damage or steal data from computer systems. Ransomware attacks, like those from Cryptolocker, TeslaCrypt, and WanaCrypt, encrypt an organization's data and demand a ransom for decryption, leading to substantial operational disruptions and financial losses (Hammouchi, et al., 2019). Phishing attacks trick individuals into providing confidential information by impersonating trustworthy entities in electronic communications, while social engineering manipulates people into breaking standard security

practices to gain access to systems or data. Insider threats, posed by employees, contractors, or business associates with access to critical data, can result in intentional or unintentional misuse. Accidental data breaches often occur due to human error, such as misconfigured databases, improper encryption, or lost devices, leading to unintentional exposure of sensitive information (Cheng, et al., 2017). The Desjardins Group breach, caused by an employee, is a notable example of an insider threat that affected 2.9 million members (Smith, 2019). These threats can have severe consequences, including financial losses, legal implications, and damage to an organization's reputation. To effectively mitigate these threats, organizations must adopt comprehensive cybersecurity measures, such as robust encryption, regular security audits, employee training, and incident response plans (Sharma, et al., 2020).

### **2.8.2 A History of Data breaches**

Data breaches have become a major concern for organizations globally, with attackers using diverse techniques to compromise data security from 2004 to 2021. These breaches have impacted millions of users, resulting in substantial financial and reputational consequences. For this report, we analyzed the most prevalent data breach methods during this period, highlighting the increasing complexity and frequency of such incidents. The dataset utilized for this analysis was obtained from Kaggle, providing a comprehensive list of the top data breaches that occurred within this timeframe (Kaggle, 2021). The visualizations presented below offer insights into the companies most affected, as well as the methods employed in these breaches.

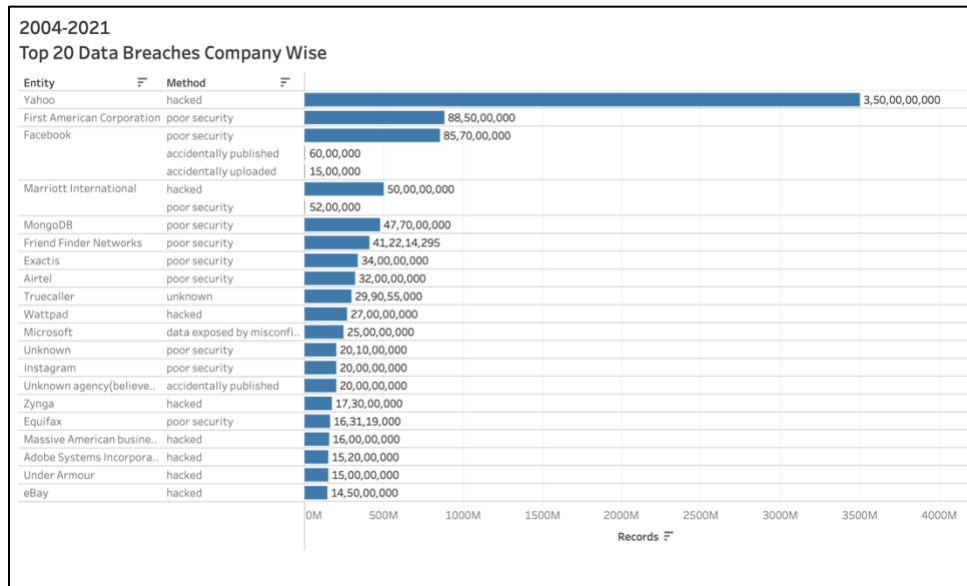


Figure 3: Top 20 data breaches by company

Figure 3 showcases the top 20 data breaches by company. Notably, Yahoo stands out as the frontrunner, having suffered a staggering 3.5 billion records breached due to hacking. This highlights the significant vulnerability even large enterprises face. The chart not only emphasizes the affected entities but also reveals the variety of methods used to execute these breaches. Alarmingly, breaches stemming from poor security measures are commonplace, underscoring the pressing need for robust cybersecurity practices. Facebook, with multiple incidents, underscores issues with both inadequate security and accidental data exposure, leading to substantial data leaks.

Additionally, Microsoft features prominently on this list, with a significant data breach resulting from data exposed by misconfiguration. Specifically, a misconfiguration of Microsoft's internal customer support database in January 2020 exposed 250 million records. This breach was caused by improper security settings, allowing unauthorized access to sensitive data such as email addresses, IP addresses, and support conversations. This incident emphasizes the critical necessity for proper configuration, regular security audits, and robust access controls to prevent such vulnerabilities.

Overall, the visualization indicates that companies must implement comprehensive cybersecurity measures, including frequent audits and employee training, to safeguard against diverse threats.

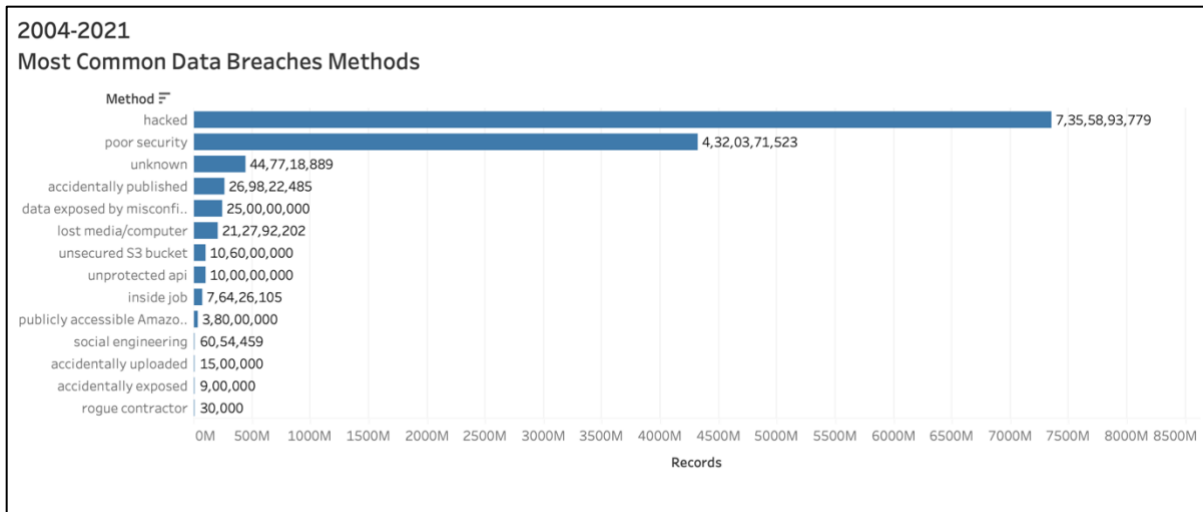


Figure 4: Most common data breach methods

Figure 4 highlights the methods used in these data breaches. It is clear from this chart that hacking remains the most prevalent technique, accounting for 7.36 billion compromised records. Following hacking, poor security practices have led to 4.32 billion records being breached. Other significant methods include unknown techniques, accidental publication, and data exposure due to misconfiguration.

### 2.8.3 Impact of Hacking, Poor Security, and Misconfiguration

Hacking is the most common method employed in data breaches, affecting billions of records. Hackers exploit vulnerabilities in software and network systems to gain unauthorized access to sensitive information, resulting in severe financial losses, reputational damage, and loss of customer trust. Companies must continually update their security protocols and invest in advanced cybersecurity technologies to protect against hacking attempts (World Economic Forum, 2023) (Sobers, 2024).

Weak security practices, such as poor passwords, lack of encryption, and insufficient access controls, significantly contribute to data breaches. Implementing robust security policies, conducting regular security audits, and ensuring proper system configuration can help mitigate these risks. Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Single Sign-On (SSO) are critical measures that can significantly enhance security. RBAC ensures that employees only have access to the data necessary for their roles, minimizing the risk of unauthorized access. MFA adds an extra layer of security by requiring multiple forms of

verification before granting access, while SSO simplifies the authentication process and reduces the likelihood of password-related breaches (World Economic Forum, 2023) (Sobers, 2024).

Misconfiguration, another major cause of breaches, occurs when default settings are not changed, sensitive data is left unprotected, or access controls are improperly set up. Regular audits and automated tools can help identify and fix misconfigurations, reducing the risk of data breaches (Winder, 2020). Educating employees about cybersecurity best practices is crucial, covering areas such as recognizing phishing attempts, using strong passwords, and understanding data handling protocols. Regular training sessions and updates on the latest threats can empower employees to act as vigilant protectors of company data (World Economic Forum, 2023) (Sobers, 2024).

## **2.9 Overview of Role-Based Access Control (RBAC) in Healthcare**

Role-Based Access Control (RBAC) is a crucial security approach used in the healthcare industry to manage and restrict access to sensitive information based on an individual's role within the organization. This method enhances security by ensuring that employees only have access to the data necessary for their job functions, thereby minimizing the risk of unauthorized access and data breaches.

RBAC operates by assigning specific roles to users, with each role having predefined permissions that dictate what information and systems the user can access. In the healthcare context, these roles typically include doctors, nurses, administrative staff, and IT personnel, with access levels tailored to their respective responsibilities. For instance, a doctor may have access to a patient's entire medical history, while administrative staff may only be able to view billing information (GoodX Healthcare, 2020) (Laviola, 2023).

One of the primary benefits of RBAC in healthcare is its ability to streamline compliance with regulations such as HIPAA and GDPR. By restricting access to sensitive patient information, RBAC helps healthcare organizations protect patient privacy and avoid costly fines and penalties associated with data breaches (Zhang, 2023). Additionally, RBAC simplifies the auditing process, allowing administrators to track who accessed specific information and when which is essential for maintaining accountability and transparency.

RBAC also improves operational efficiency by reducing the administrative burden associated with managing access permissions. When an employee changes roles or leaves the organization, their access permissions can be easily updated or revoked, reducing the risk of privilege creep where employees retain access to data they no longer need (McCarthy, 2024).

Implementing RBAC involves several key steps, including defining roles within the organization, assigning appropriate permissions to each role, assigning roles to users based on their job responsibilities, and conducting regular audits to ensure that access permissions are up-to-date and that there are no unnecessary privileges granted.

In addition to enhancing security and compliance, RBAC can also reduce the need for extensive IT support by automating the management of user permissions, leading to significant cost savings and a reduction in human error, further enhancing the overall security posture of the healthcare organization (Laviola, 2023).

RBAC is an effective and efficient method for managing access to sensitive information in healthcare. By aligning access permissions with job responsibilities, healthcare organizations can protect patient data, ensure regulatory compliance, and improve operational efficiency. Regular audits and proper implementation are critical to maintaining the integrity and effectiveness of an RBAC system.

## **Chapter 3.0: Methodology and Approach**

As we examine the nuanced nature of managing security and administration within Power Platform environments, it is crucial to recognize the potentially catastrophic consequences of data breaches and leaks, especially given their far-reaching impact on the global business landscape. To mitigate these risks, this capstone project investigates data security within this dynamic ecosystem and develops an application for a practical use case in the healthcare industry. By analyzing this scenario and the development process, this report aims to provide both technical and non-technical business teams with the insights needed to make informed decisions regarding data security and compliance, thereby ensuring a robust and secure ecosystem during organizational expansion. This sets the stage for the detailed methodology and approach used in our investigation and development.



### **3.1 Synthetic Relational Databases and Simulated Data**

To address these security challenges, organizations are increasingly turning to synthetic data and simulation techniques. Tools such as Mockaroo and Faker, along with various open-source libraries, enable the creation of synthetic relational databases that mimic real-life data characteristics. These synthetic datasets are particularly useful for testing and validating Role-Based Access Control (RBAC) concepts and user roles without exposing actual sensitive data. This approach not only enhances security but also ensures compliance with data protection regulations like General Data Protection Regulation (GDPR) (Gilli, 2023).

### **3.2 Simulated Sharing Scenarios and Synthetic Activity Logs**

In the realm of sales and operational data, simulating sharing scenarios using platforms like Power Apps can help organizations understand and mitigate the risks associated with data sharing. Synthetic activity logs generated during these simulations provide valuable insights into user behaviors and potential vulnerabilities. These logs can be instrumental in developing and refining data governance policies, ensuring that data is accessed and used appropriately within the organization (Poole, 2018).

### **3.3 Data Governance and Financial Data**

Effective data governance is crucial for managing anonymized customer data in compliance with GDPR. Organizations need to implement stringent policies and procedures to ensure that customer data is protected and used responsibly. Synthetic data can play a vital role in this process by providing realistic datasets for testing and training purposes without risking actual customer information (European Commission, 2024).

Additionally, the management of financial and transactional data requires robust security measures. Synthetic data generation allows organizations to create realistic financial datasets for analysis and testing, helping to identify and address potential vulnerabilities in their financial systems (Lamberti, 2023).

By leveraging synthetic data, simulated scenarios, and comprehensive data governance frameworks, organizations can better prepare for and mitigate the risks associated with data breaches and unauthorized access.

### **3.4 Chosen Strategy**

To address the different types of data threats that are possible within the power platform environment, it is important to learn the nuances of the power platform itself. Therefore, the first step to be implemented will be to learn the exact functioning of the power platforms, and in particular the Power Apps platform.

It is then imperative to test the understanding and possible data breaches in a real-life environment. To do this firstly the background of the implementation will be studied, followed by the implementation of the security protocols in a real-life manner through a case study, the details of which are given later in section 4.5. It is also important to be able to communicate these possible data breaches and how to get around them to the main audience of power platforms: citizen developers. Therefore, we are also looking at implementing a chatbot to answer the questions about security concerns that a potential citizen developer will have, in addition to documentation explaining the various breaches and potential security measures in a way citizen developer can understand.

The scope of this project is the analysis of security threats and risk mitigation in the power platform environment. This strategy was chosen because it provides a comprehensive approach to learning, testing and communicating security measures.

### **3.5 Advantages of Methodology**

There are many advantages to the chosen strategy, which helps in finding out the potential security breaches in power platforms, such as:

- **Comprehensive platform-specific knowledge:** By deeply learning the functioning of the power platform, we gain valuable platform-specific insights. This understanding is crucial for identifying unique vulnerabilities, and crafting tailored security measures.

- Testing security measures through realistic scenarios such as case studies ensures that security strategies are practical and effective. It also validates effectiveness and highlights areas of improvement.
- Developing documentation to communicate the findings to citizen developers in a language they will understand ensures that they receive guidance in an accessible manner. This increases the likelihood that people adhere to best practices.
- This strategy addresses both the technical and people aspects of security, which reduces the likelihood of security breaches due to human error or a lack of knowledge.

### 3.6 Limitations of the Methodology

However, there are some limitations to this strategy, such as:

- Time and resource intensive: The process of thoroughly understanding the power platform and conduct extensive testing, can be time consuming.
- Synthetic data limitations: Although synthetic data is valuable for testing, it may not capture all the complexities and nuances of real-world data.
- Developing and maintaining, security measures, as well as creating educational tools like chatbots, requires a high level of expertise in both cybersecurity and power platform.
- Ensuring that citizen developers effectively engage with and utilize the tools provided, such as the documentation and chatbot, can be challenging. Continuous training and support are required to ensure that the protocols are adhered to.

## Chapter 4.0: Objectives and Deliverables

In order to ensure that data leaks and breaches are kept to a minimum while scaling up power platforms, there needs to be certain steps taken, like maintaining robust security compliance and minimizing risk exposure are critical priorities for organizations leveraging the Power Platform. To address these challenges, we propose a comprehensive approach focused on enhancing security measures, conducting proactive risk assessments, and developing resilient response strategies. The

following outlines our detailed approach, aimed at safeguarding sensitive data, ensuring regulatory compliance, and fortifying the overall security posture of the organization.

## **4.1 Enhancing Security Compliance**

### **1. Access Controls Implementation:**

- a. Explore and implement Role-Based Access Control (RBAC) to restrict access based on user roles and responsibilities.
- b. Use of conditional access policies to enforce multi-factor authentication and other security measures based on user risk profiles.

### **2. Encryption and Data Protection:**

- a. Research on encryption of sensitive data both at rest and in transit to protect against unauthorized access.
- b. Explore and Implement Data Loss Prevention (DLP) policies to prevent the unauthorized sharing of sensitive information.

### **3. Monitoring and Auditing:**

- a. Set up monitoring and auditing tools to track and log access and changes to sensitive data.

## **4.2 Risk Reduction**

### **1. Risk Assessments:**

- a. Learn different components of the power platform (PowerBI, Power Apps, Automate, etc) and conduct risk assessments to identify vulnerabilities.

### **2. Implementation of Controls:**

- a. Apply and write on appropriate security controls such as IP firewalls, intrusion detection systems to mitigate identified risks.

### **3. Contingency Planning:**

- a. Develop and test incident response and disaster recovery plans to ensure quick recovery from potential incidents in different platform components.

## 4.3 Modelling Potential Data Breaches with Practical Case Study in Healthcare Industry

### 1. Simulation of Data Breach Scenarios:

- a. Develop and run simulations of various data breach scenarios to understand their impact on operations, reputation, and compliance within a healthcare environment.
- b. Use synthetic and transactional data to create realistic scenarios for testing, reflecting common and emerging threats.

### 2. Impact Analysis:

- a. Analyze the consequences of simulated data breaches to the healthcare organizations involved, focusing on patient data, operational disruption, and regulatory compliance like GDPR and HIPAA.
- b. Evaluate the impact of security measures like RBAC, DLP, and Conditional Access Policies on preventing data leaks.

### 3. Response Strategy Development:

- a. Develop strategies for preventing, detecting, and responding to data breaches based on simulation results.
- b. Incorporate response protocols, communication plans, handling of patient details and recovery procedures tailored for healthcare settings.

## 4.4 Comprehensive Documentation and Training

### 1. Development of Comprehensive Documentation:

- a) A thorough literature review to create detailed documentation comprising Power Platform components, security best practices, data handling procedures, compliance requirements, governance frameworks, RBAC implementation, DLP policies, and security measures.
- b) Develop training guidelines on best practices tailored for non-technical business teams, simplifying complex security concepts. (Include infographics, pictures, screen screenshots)

### 2. Continuous Improvement:

- a) Establish a feedback loop to gather user feedback and refine documentation and training materials continuously.

- b) Conduct peer reviews by Power Platform experts to ensure accuracy and relevance.

## 4.5 Success Metrics for Case Study and Capstone

The primary success metrics for the capstone project are designed to ensure robust security and efficient security as organizations expand their use of the Power Platform. The success metrics is measured upon development of the model through Power Apps, simulating a practical healthcare scenario. It is a combination of qualitative and quantitative measures and highlighted below:

1. Enhanced Compliance with Security Regulations: Ensuring compliance with relevant data protection and security regulations, such as GDPR and HIPAA, is crucial. Success will be measured by the ability of the platform to consistently meet these regulatory requirements and will be used in the healthcare case study.
2. Reduction in Data Breaches and Unauthorized Access Incidents: Success will be shown by fewer data breaches and unauthorized access incidents of the dataverse, tracked through security audits, access log monitoring of the simulation.
3. Increased Overall Security Posture: Evaluated through regular security assessments, Risk Assessment Scores, and penetration testing. A composite Overall Security Posture Rating, like Microsoft's Secure Score, will provide a comprehensive security assessment.
4. Effectiveness of Recovery Plans: The ability to respond swiftly and effectively to security incidents is a critical success factor. Metrics will include the time taken to respond to breaches, the efficiency of recovery processes, and the outcomes of incident response drills.

These metrics will be evaluated through a combination of quantitative and qualitative methods, including security audits, compliance checks, user surveys, and performance reviews of security protocols and incident response plans. By achieving these objectives, the capstone project aims to create a secure and well-governed environment for the Power Platform, enabling organizations to confidently and securely scale their digital solutions.

# Chapter 5.0: Data security Case Study: A Healthcare App

In the rapidly evolving healthcare industry, the efficient and secure management of patient information is paramount. With the advent of digital transformation, healthcare providers are increasingly leveraging technology to streamline operations, improve patient care and ensure compliance with stringent data protection laws. Keeping this in mind, it was decided to demonstrate, review and improve upon the security features of the Power Platform environments by creating a healthcare app on Power Apps and Dataverse, leveraging the security features of the Power Platform environments.

There are multiple objectives of creating the healthcare app: to streamline the workflow for healthcare professionals, ensure the security and privacy of patient data, and comply with industry standards and regulations such as GDPR and HIPAA. In addition to that, it aims to address the inefficiencies and data management issues prevalent in traditional healthcare systems. To achieve this, the app leverages the advantages of the Dataverse, as well as Role Based Access Control (RBAC). By ensuring that each user role in the organization has appropriate access to patient data, it enhances security and usability.

In the following section, we will delve deeper into Power Apps and Dataverse, exploring the foundation about the technology stack underpinning this app, and how these platforms facilitate this case study.

## 5.1 Power Apps

Power Apps is a suite of apps, services and connectors, as well as a data platform, that provides a rapid development environment to build custom apps for business needs. Developed by Microsoft, Power apps enables users to create tailored applications without requiring extensive programming knowledge, leveraging a low-code/no code approach (Microsoft, 2023). This platform integrates seamlessly with other Microsoft services such as Office 365, Azure and other third-party sites. These facilities advocate for the seamless data management capabilities that a healthcare app must have, and thus is very suitable for the case study.

## 5.2 Dataverse

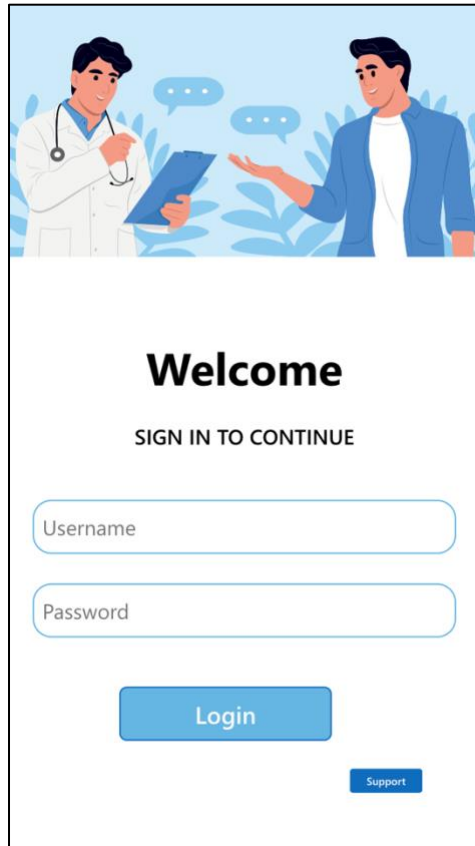
Dataverse, formerly known as the Common Data Service (CDS) is a scalable data platform used to store and manage data securely in the cloud. It is a core component of the Microsoft Power Platform, providing a unified and standardized data schema that simplifies the integration and interaction of data across various applications and systems (Microsoft, 2023).

The data stored within Dataverse is stored within a set of tables. A table is a set of rows (formerly referred to as records) and columns (formerly referred to as fields/attributes). Dataverse includes a base set of standard tables that cover typical scenarios, but custom tables can be created as well. The tables can then be populated using Power Query, and then integrated with the app so that the app can use the data (Microsoft, 2023).

In this case study, the Dataverse can be used to store different types of information, such as the different roles and their details within the organization, and storing any incident occurrences that are flagged, thereby protecting the security of the data. The data in the Dataverse is encrypted, both during storage and transportation between services, thereby making it ideal for storing the patient information. Let us now explore the different roles that the case study requires and has implemented, in the section below.



## 5.3 App User Interface



*Figure 5: Login page of the app*

The app's User Interface (UI) is designed such that it meets the diverse needs of the different roles required in the healthcare sector, while at the same time ensuring information security. The key principles guiding the UI include simplicity, clarity and accessibility, ensuring the users can navigate the app with minimal training. This is very important because many of the app's users will not be technically proficient. As one of the objectives of the project is to ensure the security features of power platform environments are accessible to people who are not technically proficient, this is an ideal approach.

The different roles in the app are accessed through a login page which is shown in Figure 5. Based on the different roles in the app, there are different screens designed, so that each role is only given the information that they need.

## 5.4 Roles implemented in the case study

In the healthcare app, different user roles are implemented to ensure that access to patient data and system functionalities is tailored according to the responsibilities and needs of each role. The various roles explored in the app are:

### 1. Directors and Executives

- **Role Description:** They oversee the strategic and operational aspects of the healthcare facility.
- **App features:** This role has to access data to aggregate data and analytics, including patient flow, resource utilization etc. They do not access individual patient records but can view anonymized data for reporting and decision-making purposes.

### 2. Doctors

- **Role Description:** Doctors are the primary caregivers, responsible for diagnosing and treating patients.
- **App features:** Doctors have full access to all patient records, including lab records, prescriptions, treatment plans etc. The app allows doctors to write and update prescriptions and make diagnostic notes.

### 3. Pharmacists

- **Role Description:** Pharmacists are responsible for managing the dispensation of medicines, ensuring the accuracy of prescriptions, and providing drug-related information to both patients and healthcare professionals.
- **App features:** They have access to the patients' prescriptions, as well as the medicine inventory of the hospital pharmacy. They can update the inventory numbers of each medicine as they are supplied to the hospital, and help in dispensing the medicines to patients as their prescriptions come in.

### 4. Receptionists

- **Role Description:** They are responsible for patient check-ins, scheduling appointments and handling initial patient queries.

- **App features:** They have access to basic patient information such as their appointment status and are able to facilitate new patient registrations. They are also able to link their bills to the patients in the database, ensuring transparency.

## 5.5 How is RBAC implemented?

In the app, RBAC is implemented using a login screen that takes in a username and password. The app has different screens connected to different user roles, which are in turn all connected to the same database in Dataverse. The screens filter out the information that is supposed to be presented to the appropriate user role and displays it in the appropriate user's screen. When a user logs in using their credentials, the app maps the credentials to the appropriate user role and displays the relevant screen. It is not possible to travel between two screens of different user roles.

The different user roles and their credentials are given below.

1. Directors and executives
  - **Username:** Executive\_01
  - **Password:** Director01
2. Doctors
  - **Usernames:** User-doctor01, User\_doctor02
  - **Passwords:** Doctor01, Doctor02
3. Pharmacists
  - **Usernames:** User\_pharmacist01, User\_pharmacist02
  - **Passwords:** Pharmacist01, Pharmacist02
4. Receptionists
  - **Usernames:** User\_recep01, User\_recep02
  - **Passwords:** Reception01, Reception02

These credentials, coupled with the different screens present in the app's User Interface (UI) work together to make the RBAC work in the app.

## 5.6 Multi Factor Authentication

In regard to the implementation of MFA in the case study, several challenging circumstances hindered the process. Specifically, under the Microsoft – University College Dublin Tenant agreement, students were restricted to a certain level of access, preventing them from modifying or creating security protocols. This limitation meant that MFA, although essential for modern technological frameworks and providing an extra layer of security, could not be tested or implemented in the healthcare app.

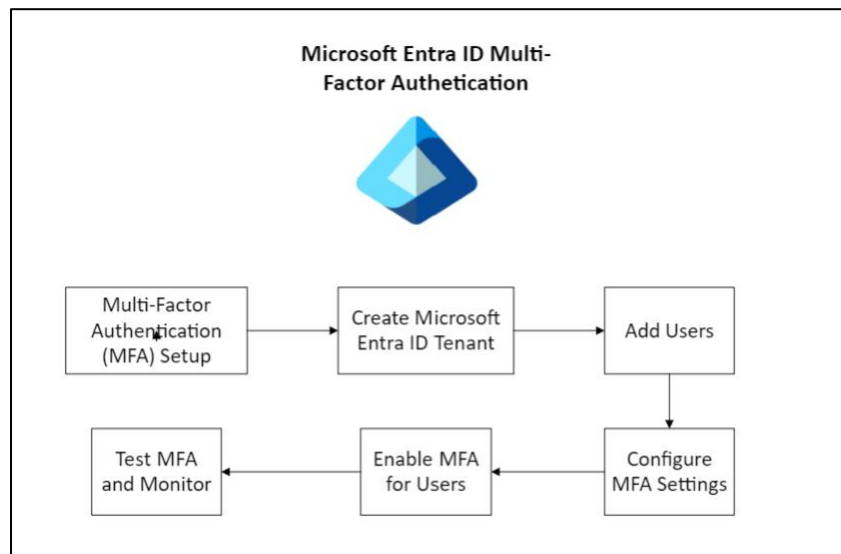


Figure 6: Multi-Factor Authentication Setup (Justinha, 2023)

Despite these constraints, it's important to acknowledge that MFA is crucial for protecting sensitive healthcare data. The implementation and setup steps outlined in Figure 6 would have been followed to ensure the successful deployment of MFA within the Power Platform, provided the necessary authority was granted. This situation underscores the importance of having appropriate administrative permissions to enforce security measures effectively.

Furthermore, this case highlights the stringent security measures enforced by Microsoft, which restrict changes to security settings to only system administrators within an organization. While these restrictions aim to safeguard the overall integrity and security of the tenant environment, they can also pose challenges when flexibility and broader access are needed for specific projects or use cases. Ensuring that the right balance is struck between security and operational flexibility is critical for organizations, especially in sensitive sectors like healthcare.

## 5.7 Single Sign On

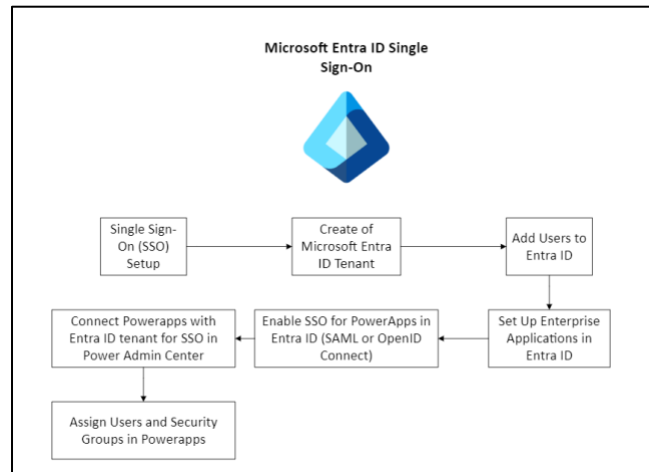


Figure 7: Single Sign-on setup (Shukla & Jain, 2016)

Similar to MFA, due to the Microsoft – University College Dublin Tenant agreement, SSO was not implemented in this healthcare scenario. However, the usual setup of Single Sign-On in Microsoft Entra ID for Power Platform is shown in Figure 7. Organizations are required to create an Entra ID tenant to add users. A further step is required compared to MFA, where administrators need to set up enterprise applications to enable SSO for their preferred Power Platform app. Administrators can define conditional access policies to control when and how users authenticate via SSO. These policies can be based on various factors such as user location, device compliance, and risk level.

In this scenario, SSO is to be enabled as OpenID connect (OAuth 2.0) in PowerApps; therefore, users, based on their security groups, are added to SSO in Entra ID.

## 5.8 Implementation of Security Groups

In this healthcare project, a security framework was implemented using roles within the Power Platform to manage access to critical data in the Dataverse. Although various roles were defined for different user types within the organization, this proof of concept focuses on three specific roles: Pharmacist, Junior System Administrator, and Senior System Administrator as shown in figure 8. This can be expanded to include other roles as needed.

Role	Business unit	Managed	Modified on ↓
Pharmacists	*** org377da026	No	08/06/2024 10:45 PM
Senior_Administrator	*** org377da026	No	08/06/2024 10:35 PM
Junior_System_Administrator	*** org377da026	No	08/06/2024 10:34 PM

Figure 8: Security Roles in Healthcare Scenario

### 5.8.1 Pharmacist – Hospital Employee

The Pharmacist role was designed to provide access to the **inventory table** within the Dataverse, which is utilized for managing medicine stocks. Given the presence of multiple pharmacists within the organization, this role was assigned to a security group in the Power admin centre as a team. Figure 9 shows the configuration and ensures that all pharmacists automatically inherit the same permissions, enabling them to read, create, and append inventory consistently. The role includes permissions to create new inventory records. It can also include the deletion of records to prevent accidental data loss, thereby maintaining the integrity of medicine records, HIPAA and GDPR compliance.

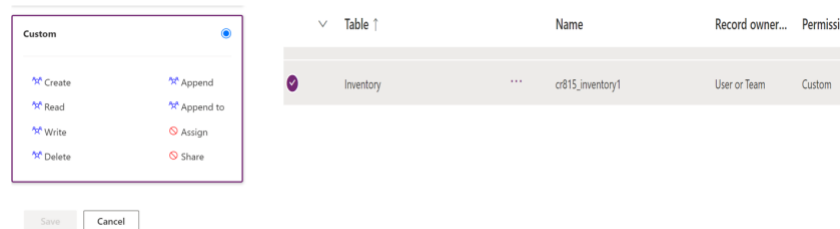


Figure 9: Pharmacist Role Permission Access Controls

### 5.8.2 Junior System Administrator – IT Systems

The Junior System Administrator role focuses on managing access to the **admin table**, which contains sensitive information such as usernames and passwords. This role was assigned as a business unit group within the Power Platform to accommodate the potential number of junior administrators. As shown in figure 10, permissions granted to this role include the ability to create, read, and write data in the admin table, enabling junior administrators to manage user credentials effectively. However, deletion of records is restricted to protect critical data from accidental or unauthorized removal, ensuring that only the senior officials have deletion access.



Figure 10: Junior System Administrator Role and Permission Controls

### 5.8.3 Senior System Administrator – IT Systems

The Senior System Administrator role was established with full access to the admin table, for for managing system security, usernames and passwords. This role includes permissions to create, read, write, and delete records within the admin table, reflecting the senior administrators' responsibility for overseeing the organization's security settings. This can be seen in figure 11. Due to the sensitivity of this role, it was assigned at the organization level and limited to a few trusted individuals, ensuring that significant changes to security configurations are made only by authorized personnel.

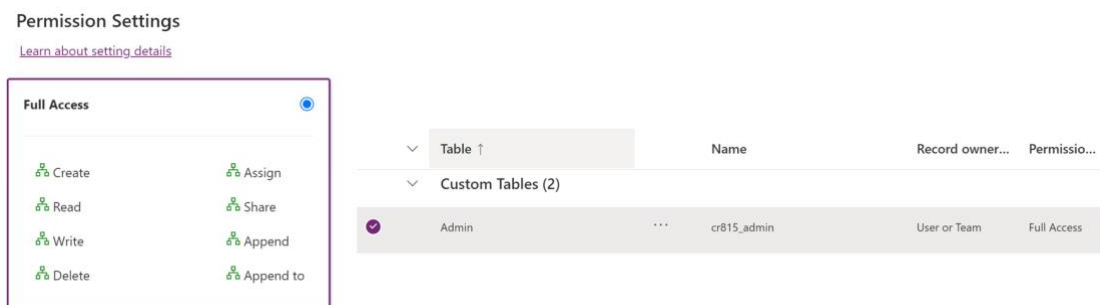


Figure 11: Senior System Administrator and Permission Access Controls

## Chapter 6.0: Working of the App

The different roles in the app are accessed through a login page which is shown in Figure 5. Based on the different roles in the app, there are different screens designed, so that each role is only given the information that they need.

## Directors and Executives

Directors and executives of the organization are responsible for overseeing the strategic and operational needs of the healthcare facility. They will have access to all the data of the departments in aggregate format, which will help them in making decisions on the operations of the organization.

## Doctors

The doctor role requires that they have access to all of their patients' information to make an informed decision regarding their diagnosis. There are a few screens dedicated to the doctor role.

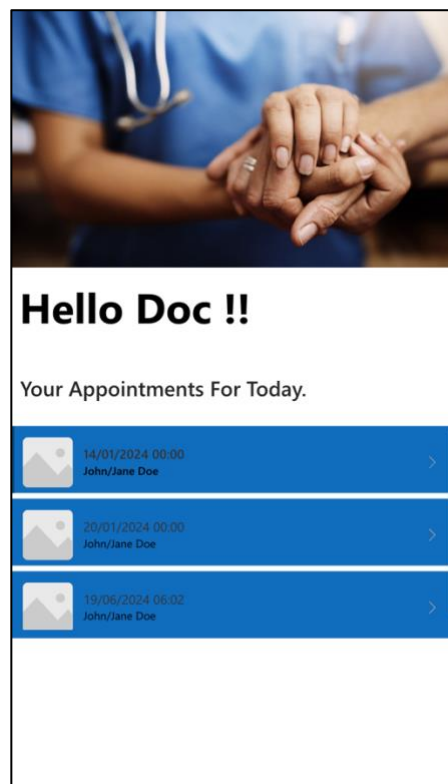
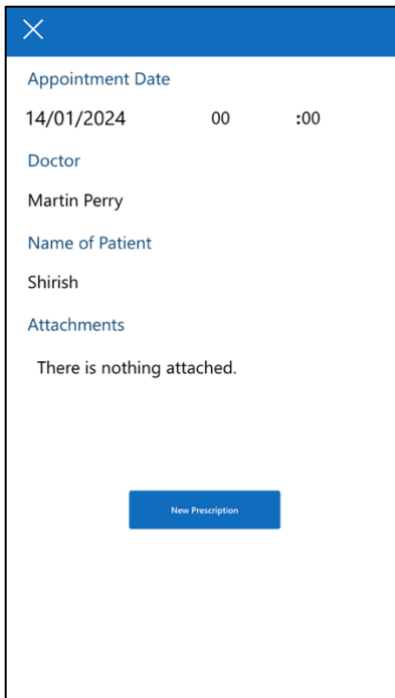


Figure 12: Doctor's Page

The first screen upon logging in to the doctor's role shows the doctor the appointments for the day, along with the date and time information of the appointments. These links are clickable, and when clicked, it switches to a page that gives more details about the selected patient.





A screenshot of a mobile application interface for a doctor's patient details page. The page has a blue header bar with a white 'X' icon in the top left corner. Below the header, the page is divided into several sections. The first section is titled 'Appointment Date' and displays '14/01/2024' followed by '00' and ':00'. The second section is titled 'Doctor' and displays 'Martin Perry'. The third section is titled 'Name of Patient' and displays 'Shirish'. The fourth section is titled 'Attachments' and displays the text 'There is nothing attached.' At the bottom of the page, there is a blue button with the text 'New Prescription'.

Appointment Date		
14/01/2024	00	:00

Doctor

Martin Perry

Name of Patient

Shirish

Attachments

There is nothing attached.

New Prescription

*Figure 13: Doctor's Patient Details Page*

The second screen, in addition to providing details about the appointment with the patient, also has a button to create a new prescription for the patient. When clicked, it opens a link to add or click a picture, as below.

Appointment Date

14/01/2024 00 :00

Doctor

Martin Perry

Name of Patient

Shirish

Attachments

There is nothing attached.

New Prescription

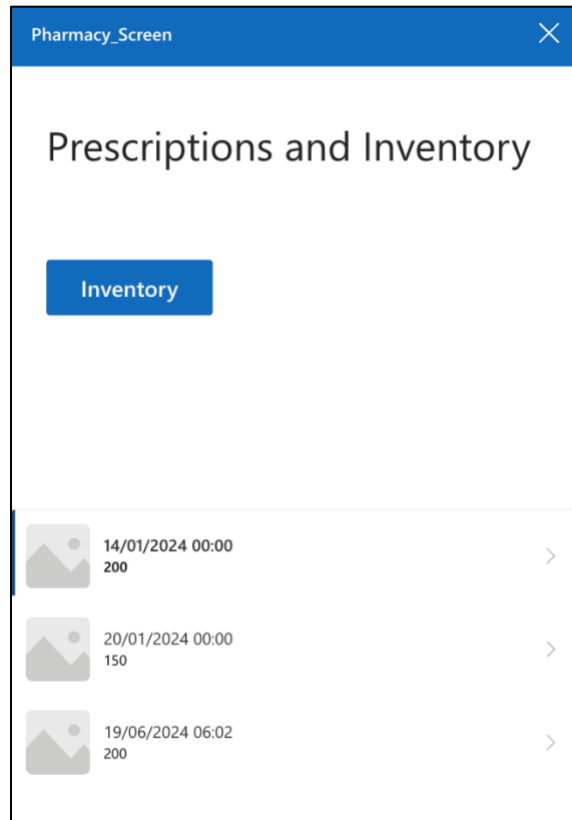
Tap or click to add a picture

*Figure 14: Doctors - Uploading Prescriptions*

Upon clicking the button, it opens up a dialogue box to open or upload a file. This way, a doctor can manage every aspect of their patient's diagnosis using this app, through the permissions assigned to their role.

## **Pharmacists**

The pharmacist role requires that they be able to access the patients' prescriptions, in order to dispense them. In addition to that, they will also be responsible for the entire stock of medicines of the organization, which will be contained in the hospital pharmacy. In view of this, there are a few screens dedicated to the pharmacists' role, as given below.



*Figure 15: Pharmacist's page*

The first screen that a pharmacist sees, contains two pieces of information: Firstly, it contains the list of pending prescriptions of all patients of the day, in a scrollable format. These entries are clickable, and upon clicking, takes the pharmacist to a page that contains the details of the individual prescription. The other aspect of the first screen is the “Inventory” button, which takes the pharmacist to the hospital medicine inventory.

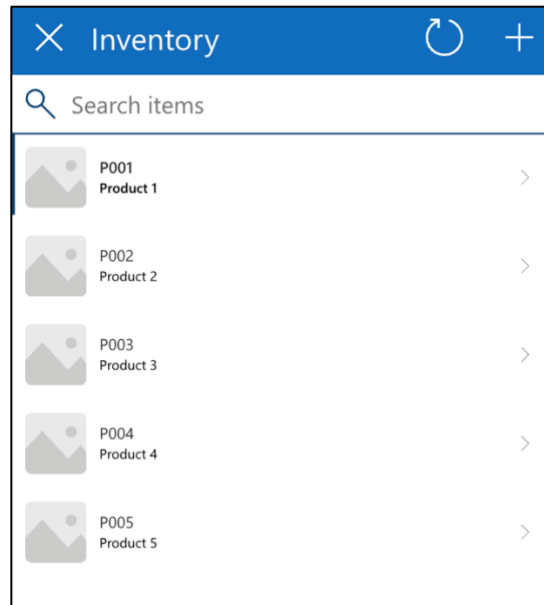


Figure 16: Pharmacists - Inventory Page

The inventory page contains a scrollable list of medicines currently available at the hospital. It also contains a search bar with which individual medicines can be searched in the database. Each of the medicines are clickable, and upon clicking, the pharmacist can update the quantities of the medicines in the inventory. The Dataverse contains the full list of medicines and can be updated as per the current stock of medicines by the pharmacist.

Product ID ↑	Created On	Product Name	Quantity	Price	Medicine C...
P001	6/15/2024 11:37 AM	Product 1	10	9.99	Category 1
P002	6/15/2024 11:37 AM	Product 2	5	19.99	Category 2
P003	6/15/2024 11:37 AM	Product 3	3	29.99	Category 3
P004	6/15/2024 11:37 AM	Product 4	8	39.99	Category 1
P005	6/15/2024 11:37 AM	Product 5	2	49.99	Category 2
Enter text		Enter text	Enter number	Enter number	Select lookup

Figure 17: Sample Inventory Table

The above picture shows the “Inventory” table in the Dataverse, which contains the quantities of each medicine in the hospital. It contains the Product ID, Product Name, Quantity of medicines, the price of medicines and the category under which each medicine comes. This enables the pharmacist to keep track of all the medicines of the hospital.

## Receptionists

The receptionist is required to handle all patients' first-time registrations, as well as any subsequent appointments with the doctors. They, however, do not need access to the patients' medical records. Keeping this in mind, receptionists have a dedicated set of screens catering to their requirements and permissions.

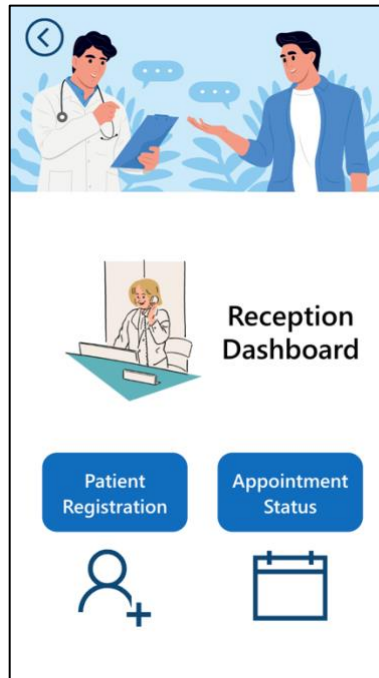


Figure 18: Receptionist's Screen

Immediately upon logging in, the receptionists see the above screen, which facilitates two tasks: new patient registration and viewing patients' appointment status. Let us look at the new patient registration screen first.

×

Patient Details

↺

✓

\* Address

Address

\* Appointment Date

31/12/2001

📅

00

⌵

:00

⌵

\* Billing Amount

Doctor

\* Email ID

\* Name of Patient

\* Transaction ID

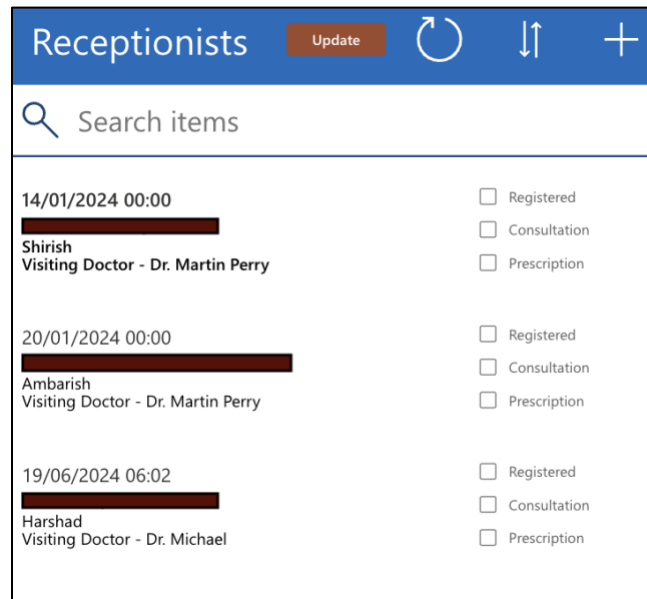
Figure 19: Receptionist - Patient Details screen

When the “Patient Registration” button is clicked, it takes the user to a form that asks for certain details about the patient, such as the address, appointment date, email ID, name of the patient, among others. The form can be filled and submitted by clicking on the “tick” button at the top right corner. Upon submission of this form, the data given will be populated into a receptionists’ patient appointments screen.

Name of Patient* ↑	Created On	Address*	Email ID*	Billing A...*	
Ambarish	6/13/2024 2:41 PM	Dublin, Ireland		150.00	1/20
Harshad	6/16/2024 3:45 PM	Point Campus, Dublin		200.00	6/15
Shirish	6/11/2024 11:51 AM	Dublin, Ireland		200.00	1/14
Enter text		Enter text	Enter email	Enter number	Enter

Figure 20: Receptionist - Sample Patient Details

The receptionist can also check the number of appointments for the day as well as look at the appointment status of the patients, by clicking the other button. Clicking the button will open a screen like below.



*Figure 21: Receptionist - Viewing Appointment Details*

Therefore, the receptionists can access and look after every aspect of the patient appointments and registrations, while at the same time not accessing the medical details of the patients.

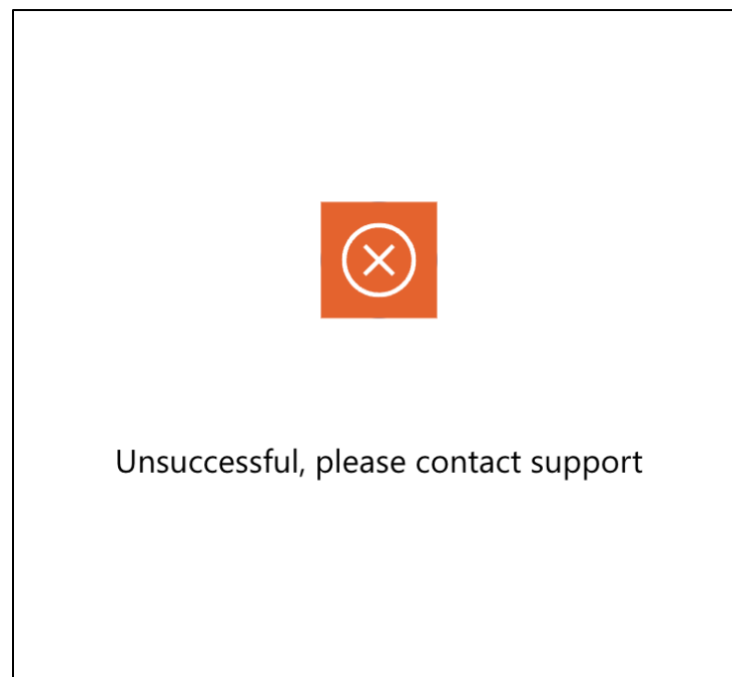
## 6.1 Data Protection feature using RBAC

The app incorporates a robust data protection strategy centered around RBAC to safeguard sensitive patient information and ensure compliance with regulatory standards such as GDPR and HIPAA. A critical component of the security feature involves managing login attempts to prevent unauthorized access. The system is designed to monitor and respond to failed login attempts, enhancing data protection.

### Login Attempt Limit

Of the given roles, the Directors/executives are given unlimited login attempts, as they are at the top management of the organization. Other roles such as receptionists, doctors and pharmacists are given a maximum of three login attempts. This will help prevent brute force attacks, where a person will try to guess the password. Directors/executives, due to their high-level access and critical

decision-making skills, do not have this login attempt restriction. However, additional security measures such as Multi-Factor Authentication (MFA) are recommended to safeguard their access.



*Figure 22: Unsuccessful Login Error Page*

When a user tries to login with incorrect credentials, the above warning will be displayed, and a counter begins to count the number of attempts made at logging in. Since Power apps is a low-code application, some aspects of creating an app can be coded using code components designed for the Canvas Apps feature of Power Apps by using Microsoft Power Platform Command Line Interface or CLI (Microsoft, 2023). Therefore, to facilitate the above warning and the subsequent disabling of logins after 3 attempts, a code is implemented on the submit button, which is given in [Appendix](#).

### **Automated alerts and account logout**

When the limit of three login attempts have been reached, a flow created in the Power Automate facility will be triggered. This is facilitated by a security patch that has been integrated into the code ([Appendix](#)). The patch records the details of the third login and creates a row in a table in Dataverse.



UserName * ↑ ↓	AttemptID * ↓	CreatedOn * ↓
123	IL-1004	7/11/2024 9:35 PM
abc	IL-1000	7/11/2024 6:19 PM
asdsad	IL-1003	7/11/2024 9:30 PM
def	IL-1001	7/11/2024 6:29 PM
esgdf	IL-1005	7/11/2024 9:40 PM

Figure 23: IncorrectLogins Table

The table “IncorrectLogins” records the details of the attempted breach, and makes a note of the date and time, and the username that was used upon the third attempt. It also creates a third parameter called “AttemptID” which is in an “Autonumber” format. An “Autonumber” format is a number format which gets automatically created by Dataverse in a user-defined format and gets assigned automatically when a new entry is made into the table. This can be used as an ID of the respective row entry of the table.

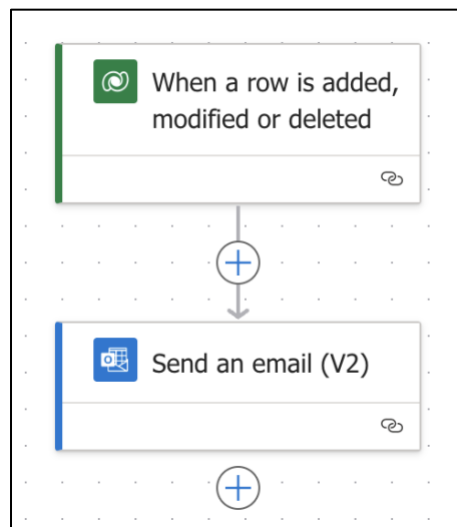
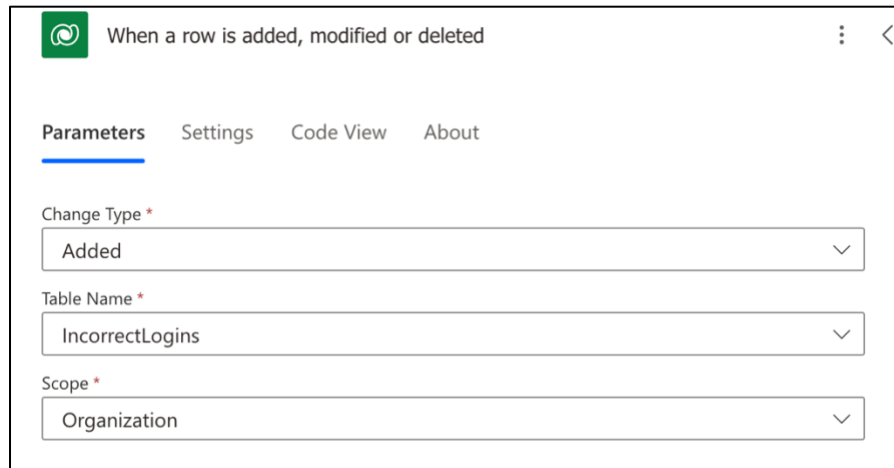


Figure 24: Email Trigger Power Automate Flow

When a new row is added to the table, a Power Automate flow gets triggered that sends an email alert to a specific email address (say, an administrator’s or director’s email address), warning that an incorrect login attempt has been made. The flow created for the purpose is depicted in the above figure.



When a row is added, modified or deleted

Parameters Settings Code View About

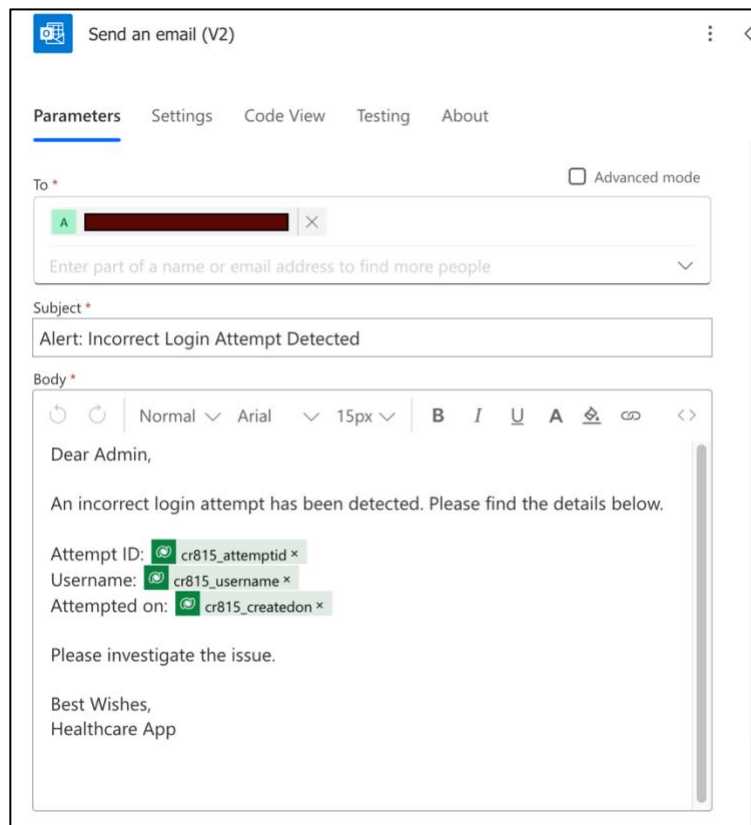
Change Type \*  
Added

Table Name \*  
IncorrectLogins

Scope \*  
Organization

Figure 25: Row Modification Details in Power Automate Flow

The first step of the flow ensures that when a new row is added to, modified, or deleted in the “IncorrectLogins” table in Dataverse, the flow will get triggered. This flow is limited to the scope of the organization as the flow parameters can potentially vary depending on the organization.



Send an email (V2)

Parameters Settings Code View Testing About

To \* ☐ Advanced mode  
A [Redacted] X  
Enter part of a name or email address to find more people

Subject \*  
Alert: Incorrect Login Attempt Detected

Body \*  
Normal Arial 15px B I U A

Dear Admin,

An incorrect login attempt has been detected. Please find the details below.

Attempt ID: cr815\_attemptid x

Username: cr815\_username x

Attempted on: cr815\_createdon x

Please investigate the issue.

Best Wishes,  
Healthcare App

Figure 26: Email Details in Power Automate Flow

When a new row is added to the table, an email alert will be sent. The parameters for the email have been shown in the above table. Dynamic values, which are values directly taken from the table “IncorrectLogins”, have been used in the email to depict the AttemptID, Username and the time and date of the attempt.

By combining RBAC with these automated security measures, the app provides a layered security approach where sensitive data is protected from unauthorized access. This system ensures that each user has appropriate access levels while protecting against unauthorized access through proactive monitoring and alerting mechanisms. This detailed approach and framework is necessary for maintaining the integrity and confidentiality of patient information in a healthcare setting.

## Chapter 7.0: Architecture of the App

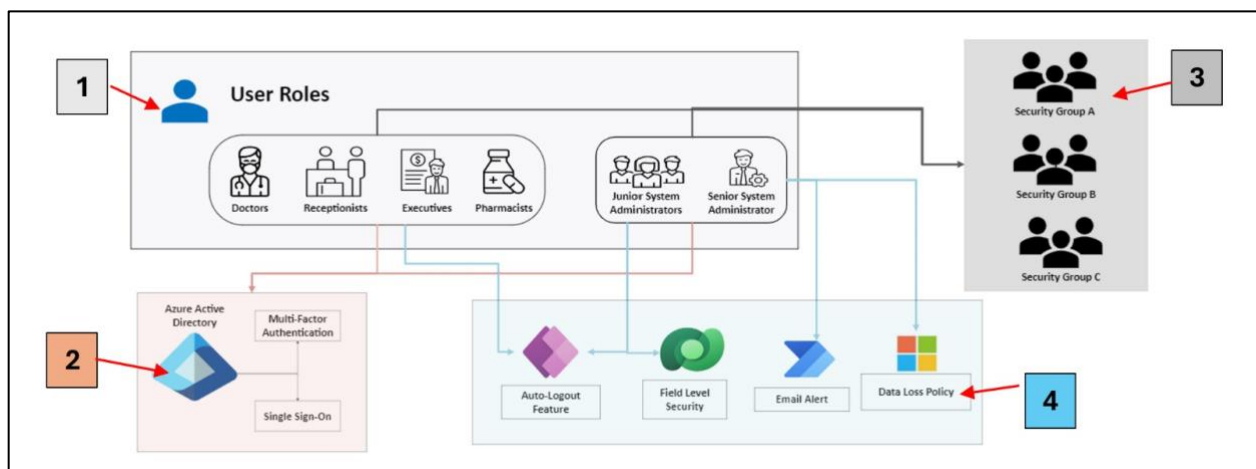


Figure 27: Architecture of the app

As mentioned earlier, the app's security is based on the different user roles that are implemented. From section 1 in Figure 21, we can see that these roles have access to different parts of the app. First, people are assigned to various security roles, as shown in section 3.

The security group comprising doctors, receptionists, executives, and pharmacists will have access to the Multi-Factor Authentication (MFA) and Single Sign-On (SSO) features of the app, which are managed by the Azure Active Directory (section 2). Since administrators need to assign roles and reset credentials when required, they will also have access to these features.

Additionally, the different user roles have restrictions on the number of login attempts, which can be reset by administrators, as depicted in the "Auto logout Feature" of section 4.

However, there are certain areas where only administrators are allowed access. Access to connectors such as Dataverse, the email alerts sent by Power Automate, and the setup of Data Loss Prevention Policies of the app are solely within the administrators' security group (section 4). This way, the different functionalities of the app are restricted to the various security groups, leveraging the role-based access control of the app.

## 7.1 Data Loss Prevention Policies

Data Loss Prevention (DLP) refers to a set of tools and strategies designed to safeguard sensitive data from being lost, misused, or accessed by unauthorized individuals. DLP systems monitor, detect, and block the movement of critical information across an organization's network. The primary purpose of DLP is to prevent unauthorized data transmission and ensure that data handling aligns with regulations and organizational policies (Microsoft, 2024) (Chia, 2023).

DLP is crucial for several key reasons:

- **Protection of Sensitive Information:** DLP ensures that sensitive data, such as personal information, financial details, and intellectual property, is not exposed to unauthorized entities. This protection is vital to prevent data breaches that can result in significant financial losses and reputational damage (Microsoft, 2024) (Baig, 2023)
- **Regulatory Compliance:** Many industries are subject to strict regulations regarding data privacy and protection, such as GDPR, HIPAA, and PCI-DSS. DLP helps organizations comply with these regulations by ensuring that sensitive data is handled appropriately and securely (Mandelecha, 2023) (Glynn, 2024).
- **Prevention of Data Breaches:** By monitoring and controlling data flows, DLP can prevent accidental or intentional data breaches. This includes unauthorized data transfer via email, cloud services, or external devices (Chia, 2023) (Microsoft, 2024).
- **Operational Efficiency:** Implementing DLP can streamline data security processes, reduce the need for manual monitoring, and enable more efficient data handling practices within an organization (Baig, 2023).

## 7.2 Implementation of Data Loss Prevention (DLP) in Our Project

In our project, we have strategically implemented DLP using the Power Platform's DLP policies. These policies are configured to manage and protect sensitive data by classifying connectors and controlling the data flow between them. Let me provide a detailed explanation of how four key business tools—Microsoft Dataverse, Power Automate Management, Power Automate for Admins, and Office 365 Outlook—are used to prevent data loss:

Assign connectors ⓘ

Business (4)

Non-business (1244) | Default

Blocked (0)

Search connectors

Connectors for sensitive data. Connectors in this group can't share data with connectors in other groups.





	Name ▾		Blockable ▾	Endpoint configu... ▾	Class ▾
	Microsoft Dataverse	⋮	No	No	Premium
	Power Automate Management	⋮	Yes	No	Standard
	Power Automate for Admins	⋮	Yes	No	Standard
	Office 365 Outlook	⋮	No	No	Standard

Figure 28: Data Loss Prevention Policy - Allowed Connectors

### Microsoft Dataverse

Role: Serves as the primary data storage and management platform, designed to securely store and manage data used by business applications.

DLP Implementation: Dataverse is classified as a 'Business' connector and is not blockable, meaning it is considered safe and essential for business operations. By ensuring that only approved connectors can interact with Dataverse, we prevent unauthorized access and potential data leakage.

## **Power Automate Management**

Role: Provides administrative capabilities to manage Power Automate environments, flows, and users.

DLP Implementation: This connector is classified as 'Business' and is blockable. This means we can restrict or allow its use based on specific DLP policies. By monitoring and controlling administrative actions, we ensure that only authorized users can make changes, thereby protecting sensitive workflows from being altered maliciously.

## **Power Automate for Admins**

Role: Offers administrative functions focused on governance and oversight of Power Automate activities.

DLP Implementation: Also classified as 'Business' and blockable, this connector allows us to enforce strict policies regarding who can perform administrative tasks. By doing so, we maintain a secure environment where administrative privileges are tightly controlled, reducing the risk of unauthorized access or configuration changes that could lead to data breaches.

## **Office 365 Outlook**

Role: Handles email communication and scheduling, integral to business operations.

DLP Implementation: As a 'Business' connector that is not blockable, Outlook is configured to ensure that email communications involving sensitive data adhere to the organization's security policies. By integrating DLP rules, we can monitor and control the flow of sensitive information, preventing it from being inadvertently shared with unauthorized parties.

The strategic classification and configuration of these connectors within the Power Platform's DLP policies enable robust protection against data loss. By ensuring that business-critical connectors like Microsoft Dataverse and Office 365 Outlook are securely managed, and by controlling administrative tools like Power Automate Management and Power Automate for Admins, we effectively safeguard sensitive data. Regular audits and compliance checks further enhance this protective framework, ensuring ongoing adherence to data protection standards and regulations.

# Chapter 8.0: Results and Conclusion

## 8.1 Results

The capstone project focused on the security and administration of Power Platform environments, particularly within the healthcare sector. Through a comprehensive literature review and practical case study, the project explored the integration of security features such as Data Loss Prevention (DLP) policies, Role-Based Access Control (RBAC), and compliance with regulations like GDPR and HIPAA. The project successfully implemented various security protocols and simulated different data breach scenarios to assess their impact and effectiveness. Here are the detailed results:

The implementation of DLP rules within the Power Platform significantly enhanced security compliance by improving the monitoring and control of sensitive data. By strategically classifying and configuring connectors, the project ensured that business-critical data was protected against unauthorized access and potential data breaches. Regular audits and compliance checks were established to reinforce adherence to data protection standards.

The project successfully demonstrated a reduction in data breaches and unauthorized access incidents through the application of RBAC, MFA and DLP policies. The healthcare app developed during the project showcased a streamlined workflow for healthcare professionals while ensuring the security and privacy of patient data.

The simulation of potential data breaches highlighted the vulnerabilities within healthcare organizations. The analysis revealed that the implementation of robust security measures could mitigate the impact of such breaches, ensuring operational continuity and compliance with regulatory requirements.

The project also focused on creating detailed documentation and training materials. These resources helped non-technical business teams understand complex security concepts, promoting a culture of security awareness and continuous improvement within the organization.

To measure the success of the project, clear metrics were established. These included better compliance with security regulations, fewer data breaches, and an overall improvement in the organization's security posture. These metrics were evaluated using both qualitative and quantitative methods, providing a thorough assessment of the project's impact.

## **8.2 Conclusion**

The project demonstrated that with proper security measures, the Power Platform could be effectively managed and secured, even in highly sensitive environments like healthcare. The implementation of role-based access control (RBAC), data loss prevention (DLP) policies, and conditional access significantly enhanced data protection and compliance. Regular monitoring, auditing, and simulated breach scenarios provided valuable insights into potential vulnerabilities and the effectiveness of the implemented security measures.

The project encountered some challenges due to restrictions from the University College Dublin tenant, which prevented the use of advanced security features like multi-factor authentication (MFA) and single sign-on (SSO). It also emphasized the need to explore better security measures in other fields such as manufacturing, IT, and finance. Moving forward, incorporating new technologies like artificial intelligence, machine learning, and data science into strong security frameworks will be vital to protect sensitive data and ensure robust security across different sectors. The next steps will focus on addressing these limitations and extending security improvements to other industries.

The detailed approach and findings of this project provide a solid foundation for enhancing security and governance within the Power Platform, paving the way for its broader application and scalability in diverse organizational settings.

## **Chapter 9.0: Future Work and Scope**

The project focuses on exploring the Power Platform and its security features. We conducted a thorough review of existing literature and applied our findings in a practical case study within the healthcare sector. Starting at a single organizational level, our study can potentially expand to encompass large global corporations with diverse departments. While our current focus was on a limited number of roles for practical reasons, future phases could include a broader array of



security roles across different departments, making our findings more broadly applicable and detailed.

Despite our achievements, we faced challenges due to limitations imposed by the University College Dublin Tenant. These constraints made it difficult to implement advanced security features such as Multi-Factor Authentication (MFA) and Single Sign-On (SSO). Looking ahead, further progress depends on obtaining clearance and authorization to implement and validate these advanced security concepts. This effort includes exploring enhanced security measures in light of emerging technologies like AI, machine learning, and data science. Moreover, these security measures should be explored in other diverse industries such as manufacturing, IT, finance, and more. Integrating these technologies with strong security frameworks will be essential for protecting sensitive data and operations across various sectors, ensuring comprehensive and robust security.

## Chapter 10.0: References

Verizon, 2024. *2024 Data Breach Investigations Report*. [Online]

Available at: <https://www.verizon.com/business/resources/reports/dbir/>

[Accessed May 2024].

Flashpoint, 2024. *Flashpoint 2024 Global Threat Intelligence Report*. [Online]

Available at: <https://flashpoint.io/resources/report/2024-global-threat-intelligence-report/>

[Accessed May 2024].

Sarabi, A., Naghizadeh, P., Liu, Y. & Liu, M., 2016. Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, 2(1), pp. 15-28.

Bock, A. C. & Frank, U., 2021. Low-Code Platform. *Business and Information Systems Engineering*, 63(6), pp. 733-740.

Vincent, P. et al., 2019. Magic Quadrant for Enterprise Low-Code Application Platforms. *Gartner Report*.

Oluwaseyi, J., 2024. A Comprehensive Overview of No-Code and Low-Code Development Paradigms.

Standefer, R. & Yack, D., 2023. *Application Modernization with Microsoft Power Platform*, s.l.: s.n.

Dataworks, n.d. *Unleash The Microsoft Power Platform: Overcoming the Challenges of Remote Working with Power Platform*. [Online]

Available at: <https://www.dataworks.ie/unleash-the-microsoft-power-platform/#:~:text=97%25%20of%20Fortune%20500%20companies,solved%20with%20the%20Power%20Platform>

[Accessed May 2024].

Okta, 2023. *Authentication vs Authorization*. [Online]

Available at: <https://www.okta.com/identity-101/authentication-vs-authorization/>

[Accessed May 2024].

OneLogin, n.d. *Authentication vs Authorization*. [Online]

Available at: [https://www.onelogin.com/learn/authentication-vs-authorization#:~:text=Authentication%20verifies%20the%20user%20\(Lucia,access%20\(view%20sales%20information\).](https://www.onelogin.com/learn/authentication-vs-authorization#:~:text=Authentication%20verifies%20the%20user%20(Lucia,access%20(view%20sales%20information).)

[Accessed May 2024].

Auth0, n.d. [Online]

Available at: <https://auth0.com/intro-to-iam/authentication-vs-authorization#>

[Accessed May 2024].

Mehta, J., n.d. *Understanding The Difference: Authentication vs. Authorization*. [Online]

Available at: <https://certera.com/blog/understanding-the-difference-authentication-vs-authorization/>

[Accessed May 2024].

Juma'h, A. H. & Alnsour, Y., 2019. The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, 28(2), pp. 275-301.

Hammouchi, H. et al., 2019. Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. *Procedia Computer Science*, Volume 151, pp. 1004-1009.

Cheng, L., Liu, F. & Yao, D., 2017. Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), p. e1211.

Smith, C., 2019. *Massive Desjardins Group data breach caused by employee who's since been fired*. [Online]

Available at: <https://www.straight.com/news/1257561/massive-desjardins-group-data-breach-caused-employee-whos-been-fired>

[Accessed May 2024].

Sharma, N., Oriaku, E. A. & Oriaku, N., 2020. Cost and Effects of Data Breaches, Precautions, and Disclosure Laws. *International Journal of Emerging Trends in Social Sciences*, 8(1), pp. 33-41.

Chik, J., 2024. *5 ways to secure identity and access for 2024*. [Online]  
Available at: <https://www.microsoft.com/en-us/security/blog/2024/01/10/5-ways-to-secure-identity-and-access-for-2024/>  
[Accessed May 2024].

Microsoft, 2022. *The Total Economic Impact Of Microsoft Power Platform Premium Capabilities*, s.l.: Forrester.

Microsoft, 2024. *Microsoft Power Platform: 2024 release wave 1 plan*. [Online]  
Available at:  
<https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fpower-platform%2Frelease-plan%2F2024wave1%2Ftoc.json>  
[Accessed May 2024].

Gilli, L., 2023. *Generating synthetic data within relational databases*. [Online]  
Available at: <https://www.clearbox.ai/blog/2023-01-30-generating-synthetic-data-with-relational-databases>  
[Accessed 28 May 2024].

Poole, D., 2018. *Realistic, simulated data for testing, development and prototypes*. [Online]  
Available at: <https://www.red-gate.com/hub/product-learning/sql-data-generator/how-to-generate-various-forms-of-realistic-data-for-testing-development-and-prototypes>  
[Accessed 28 May 2024].

European Commission, 2024. *Digital financial services: synthetic data ensures compliance with confidentiality requirements*. [Online]  
Available at: [https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/digital-financial-services-synthetic-data-ensures-compliance-confidentiality-requirements-2024-03-20\\_en#:~:text=To%20ensure%20compliance%20with%20confidentiality,firms%20while%20respecting%20](https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/digital-financial-services-synthetic-data-ensures-compliance-confidentiality-requirements-2024-03-20_en#:~:text=To%20ensure%20compliance%20with%20confidentiality,firms%20while%20respecting%20)  
[Accessed May 2024].

Lamberti, A., 2023. *Beyond GDPR: how synthetic data helps companies navigate the complexities of data protection and privacy*. [Online]  
Available at: <https://syntheticus.ai/blog/beyond-gdpr-how-synthetic-data-helps-companies-navigate-the-complexities-of-data-protection-and->

[privacy#:~:text=As%20it%20is%20generated%20from,data%20breaches%20or%20unauthorized%20access.](#)

[Accessed May 2024].

Wang, X., 2023. *Enhancing Business Processes through Dynamics Solutions with Microsoft Power Platform*, s.l.: Metropolia University of Applied Sciences.

Binzer, B. & Winkler, T. J., 2022. *Democratizing Software Development: A Systematic Multivocal Literature Review and Research Agenda on Citizen Development*. s.l., Proceedings of the 13th International Conference on Software Business (ICSOB).

Herrera, H., 2022. *Microsoft Power Platform Solution Architect's Handbook: An expert's guide to becoming a Power Platform solution architect and preparing for the PL-600 exam*. s.l.: Packt Publishing Ltd.

Wadiwala, R. & India, S., 2019. *The good, the bad and the ugly of Power Automate in 2021*, s.l.: Sogeti India.

Ajish, D., 2024. A Comprehensive Review of the Significance of Low-code Automation in Risk Management for Banks. *International Journal of Innovative Research in Computer Science and Technology*, 12(2), pp. 47-58.

Sufi, F., 2023. Algorithms in Low-Code-No-Code for Research Applications: A Practical Review. *Algorithms*, 16(2), p. 108.

Palmer, T., 2020. *Microsoft PowerApps as an Alternative Solution for Business Application Development*, s.l.: Haaga-Helia University of Applied Sciences.

Evans, W. & Petersson, B., 2023. *How does low-code development correspond with best practice in software development?*, s.l.: Malmo Universitet.

Reza, R., 2023. Dataflows. *Pro Power BI Architecture: Development, Deployment, Sharing, and Security for Microsoft Power BI Solutions*, pp. 129-155.

Gannon, D. et al., 2014. *Science in the Cloud: Lessons from Three Years of Research Projects on Microsoft Azure*. s.l., Proceedings of the 5th ACM workshop on scientific cloud computing.

Leung, T. & Leung, T., 2021. Introducing Power Apps. *Beginning Power Apps: The Non-Developer's Guide to Building Business Applications*, pp. 3-19.

Miyake, T., Yoshimasa, M., Akiko, O. & Atsushi, I., 2023. *Strategic Risk Management for Low-Code Development Platforms with Enterprise Architecture Approach: Case of Global*

*Pharmaceutical Enterprise*. Singapore, International KES Conference on Innovation in Medicine and Healthcare.

Wilhelms, J., 2024. *Azure Sandbox Manager: Enhancing Efficiency and Reducing Costs*, s.l.: Vaasan Ammattikorkeakoulu University of Applied Sciences.

Di Ruscio, D. et al., 2022. Low-code development and model-driven engineering: Two sides of the same coin. *Software and Systems Modeling*, Volume 21, pp. 437-446.

Gautam, M. & Kumar, M., 2023. *Power BI Dashboard for Analysis of Success and Failures of APIs and Average Time Taken by API to process*, Solan: Jaypee University of Information Technology.

Heine, S. et al., 2023. *Bi, Python and Low Code Applications to Accelerate Digital Transformation*. Port of Spain, Trinidad and Tobago, SPE Latin American and Caribbean Petroleum Engineering Conference.

Shukla, S. & Jain, K., 2024. Rise of Identity and Access Management with Microsoft Security. *International Journal on Advances in Engineering Technology and Science*, 5(1), pp. 2455-3131.

Deckler, G., Powell, B. & Gordon, L., 2022. *Mastering Microsoft Power BI: Expert techniques to create interactive insights for effective data analytics and business intelligence*, s.l.: Packt Publishing Ltd.

Ullrich, J., Cropper, J., Frühwirth, P. & Weippl, E., 2016. The role and security of firewalls in cyber-physical cloud computing. *EURASIP Journal on Information Security*, pp. 1-20.

Ochei, L. C., Ogunsakin, R. & Ajioka, N., 2023. A Framework for a Decision Support System to Optimize Cloud-hosted Services for Multitenancy Isolation. *International Journal of Applied Information Systems*, 12(40), pp. 22-39.

Ferry, E., O. Raw, J. & Curran, K., 2015. Security evaluation of the OAuth 2.0 framework. *Information & Computer Security*, 23(1), pp. 73-101.

Rising, P., 2023. *Microsoft 365 Security, Compliance, and Identity Administration: Plan and implement security and compliance strategies for Microsoft 365 and hybrid environments*. s.l.: Packt Publishing Ltd.

L'Esteve, R., 2022. *The Azure Data Lakehouse Toolkit: Building and Scaling Data Lakehouses on Azure with Delta Lake, Apache Spark, Databricks, Synapse Analytics, and Snowflake*. s.l.: Apress LP.

Matvitskyy, O. et al., 2023. *Magic Quadrant for Enterprise Low-Code Application Platforms*, s.l.: Gartner.

Microsoft, 2022. *Security in Microsoft Power Platform*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-platform/admin/security/overview>  
[Accessed 1 August 2024].

Barr, J., 2020. *Introducing Amazon Honeycode – Build Web & Mobile Apps Without Writing Code*. [Online]  
Available at: <https://aws.amazon.com/blogs/aws/introducing-amazon-honeycode-build-web-mobile-apps-without-writing-code/>  
[Accessed 1 Aug 2024].

Codemotion, 2022. *Understanding the Boom of Low Code and No-Code*. [Online]  
Available at: <https://www.codemotion.com/magazine/backend/software-architecture/understanding-the-boom-of-low-code-and-no-code/>  
[Accessed 1 August 2024].

Amazon, 2024. *Amazon Web Services: Risk and Compliance*, s.l.: Amazon Web Services.

Kaggle, 2021. *List of Top Data Breaches (2004-2021)*. s.l.:s.n.

World Economic Forum, 2023. *2023 was a big year for cybercrime – here’s how we can make our systems safer*. [Online]  
Available at: <https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/#:~:text=Having%20a%20formal%20cybersecurity%20strategy,challenges%20and%20improve%20digital%20trust>  
[Accessed 1 August 2024].

Sobers, R., 2024. *161 Cybersecurity Statistics and Trends [updated 2023]*. [Online]  
Available at: <https://www.varonis.com/blog/cybersecurity-statistics>  
[Accessed 1 August 2024].

Winder, D., 2020. *Microsoft Security Shocker As 250 Million Customer Records Exposed Online*. [Online]  
Available at: <https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/>  
[Accessed 29 July 2024].

GoodX Healthcare, 2020. *ROLE-BASED ACCESS CONTROL EXPLAINED (WITH AN EXAMPLE)*. [Online]

Available at: <https://www.goodx.healthcare/news/role-based-access-control-explained-with-an-example/#:~:text=But%20by%20introducing%20a%20role,system%20without%20too%20much%20consultation>  
[Accessed 29 July 2024].

Laviola, E., 2023. *The Role of Access Control Systems in Healthcare for Comprehensive Security*. [Online]  
Available at: <https://healthtechmagazine.net/article/2023/12/access-control-systems-in-healthcare-perfcon>  
[Accessed 21 July 2024].

Zhang, E., 2023. *What is Role-Based Access Control (RBAC)? Examples, Benefits, and More*. [Online]  
Available at: <https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more>  
[Accessed 25 July 2024].

McCarthy, M., 2024. *The Definitive Guide to Role-Based Access Control (RBAC)*. [Online]  
Available at: <https://www.strongdm.com/rbac>  
[Accessed 23 July 2024].

Microsoft, 2024. *Manage Data Policies*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-platform/admin/prevent-data-loss>  
[Accessed 23 July 2024].

Chia, A., 2023. *Data Loss Prevention (DLP): Definition, Components & Types*. [Online]  
Available at: [https://www.splunk.com/en\\_us/blog/learn/dlp-data-loss-prevention.html](https://www.splunk.com/en_us/blog/learn/dlp-data-loss-prevention.html)  
[Accessed 20 July 2024].

Microsoft, 2024. *Data Loss Prevention (DLP) policies*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention>  
[Accessed 1 August 2024].

Mandelecha, A., 2023. *What is Data Loss Prevention? DLP Best Practices, Use Cases & Benefits*. [Online]  
Available at: <https://www.strac.io/blog/data-loss-prevention-guide>  
[Accessed 25 July 2024].

Baig, A., 2023. *What is Data Loss Prevention (DLP) and Why Is It Important?*. [Online]  
Available at: <https://securiti.ai/what-is-data-loss-prevention-dlp/>  
[Accessed 2 August 2024].

Glynn, F., 2024. *What is Data Loss Prevention (DLP), and How Does It Work?*. [Online]  
Available at: [https://www.nextdlp.com/resources/blog/what-is-data-loss-prevention#:~:text=Data%20loss%20prevention%20\(DLP\)%20is%20a%20comprehensive%20approach%20to%20protecting,or%20accessed%20by%20unauthorized%20users](https://www.nextdlp.com/resources/blog/what-is-data-loss-prevention#:~:text=Data%20loss%20prevention%20(DLP)%20is%20a%20comprehensive%20approach%20to%20protecting,or%20accessed%20by%20unauthorized%20users)  
[Accessed 15 July 2024].

Microsoft, 2023. *What is Power Apps?*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-apps/powerapps-overview>  
[Accessed 24 July 2024].

Microsoft, 2023. *What is Microsoft Dataverse?*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-apps/maker/data-platform/data-platform-intro>  
[Accessed 15 July 2024].

Microsoft, 2023. *Code components for canvas apps*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-apps/developer/component-framework/component-framework-for-canvas-apps>  
[Accessed 25 June 2024].

Ometov, A. et al., 2018. Multi-factor Authentication: A Survey. *Cryptography*, 2(1), p. 1.

Hossain, S., Yigitcanlar, T., Nguyen, K. & Xu, Y., 2024. Local government Cybersecurity Landscape: A systematic review and conceptual framework. *Applied Sciences*, 14(13), p. 5501.

Kasahara, Y. & Shimayoshi, T., 2022. *Our design and implementation of multi-factor authentication deployment for Microsoft 365 in Kyushu University*. s.l., ACM SIGUCCS Annual Conference, pp. 55-61.

Justinha, 2023. *Enable Microsoft Entra multifactor authentication*. [Online]  
Available at: <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa>  
[Accessed 3 August 2023].

Sherstobitoff, R., 2008. Anatomy of a data breach. *Information Security Journal*, 17(5-6), pp. 247-252.



Pureti, N., 2020. Implementing Multi-Factor Authentication (MFA) to enhance security. *International Journal of Machine learning research in Cybersecurity and Artificial Intelligence*, 11(1), pp. 15-29.

Liou, J. C. & Bhashyam, S., 2010. *A feasible and cost effective two-factor authentication for online transactions*. s.l., IEEE.

Proctor, W., Storm, P., Hanlon, M. & Mendoza, N., 2017. *Securing HPC: Development of a low cose, open source multi-factor authentication infrastructure*. s.l., Proceedings of the International Conference for high performance computing, networking, storage and analysis, pp. 1-11.

Reno, J., 2013. Multifactor Authentication: Its time has come. *Technology Innovation Management Review*, 3(8), pp. 40-58.

Roopesh, M., 2024. Cybersecurity Solutions and Practices: Firewalls, Intrusion Detection/Prevention, Encryption, Multi-Factor Authentication. *Academic Journal on Business Administration, Innovation and Sustainability*, 4(3), pp. 37-52.

De Clerq, J., 2002. *Single Sign-on Architectures*. Berlin, Heidelberg, International Conference on Infrastructure Security.

Chitalia, U. et al., 2013. Single Sign-on (SSO). *International Journal of Advances in Engineering Sciences and Technology*.

Pandey, P. & Nisha, T., 2017. Challenges in Single Sign-on. *Journal of Physics: Conference Series*, 1964(4), p. 042016.

Mainka, C., Mladenov, V., Schwenk, J. & Wich, T., 2017. SoK: Single Sign-on security - An evaluation of OpenID Connect. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 251-266.

Shukla, S. & Jain, K., 2016. *Rise of Identity and Access Management with Microsoft Security*, s.l.: s.n.

Thakare, A. et al., 2020. PARBAC: Priority attribute-based RBAC model for Azure IoT cloud. *IEEE Internet of Things Journal*, 7(4), pp. 2890-2900.

Leung, T. & Leung, T., 2021. Administering Security. *Beginning Power Apps: The Non-Developer's Guide to Building Business Applications*. pp. 883-918.

Tverhasselt, 2024. *Configure Security Groups - Power Platform*. [Online]  
Available at: <https://learn.microsoft.com/en-us/power-platform/enterprise->

[templates/finance/sap-procurement/administer/configure-security-groups](#)  
[Accessed 14 August 2024].

Herrera, H., 2022. *Microsoft Power Platform Solution Architect's Handbook: An Expert's guide to becoming a Power Platform solution architect and preparing for the PL-600 exam*. s.l.:Packt Publishing Ltd.

# Appendix

## Code for Login button

```
// Validate the user login
If(
    varIsBlocked,
    Notify("You are blocked from attempting to login. Please contact support.",
NotificationType.Error),
    If(
        !IsBlank(LookUp(Admin_receptions, Username = TextInput1.Text And Password
= TextInput2.Text).Username),
        With(
            {userRole: LookUp(Admin_receptions, Username = TextInput1.Text And
Password = TextInput2.Text).Role},
            Switch(
                userRole,
                "Receptionist",
                Navigate(Reception_Screen),
                "Doctor",
                Navigate(Doctor_Screen),
                "Pharmacist",
                Navigate(Pharmacy_Screen),
                "Director",
                Navigate(Director_Screen), // Director navigates to Director
screen
                Navigate(Unsuccessful_login) // Default case if role is not found
            );
            // Reset attempts after successful login
            Set(varAttempts, 0)
        ),
        With(
            {userRole: LookUp(Admin_receptions, Username =
TextInput1.Text).Role},
            Switch(
                userRole,
                "Director",
                Notify("Incorrect password. Please try again.",
NotificationType.Error), // Directors get unlimited attempts
                "Doctor",
                If(
                    varAttempts >= 2,
                    Set(varIsBlocked, true);
                    Notify("You have been blocked after 3 unsuccessful
attempts.", NotificationType.Error);
```

```

        Patch(
            IncorrectLogins,
            Defaults(IncorrectLogins),
            {
                UserName: TextInput1.Text,
                CreatedOn: Now()
            }
        );
        Navigate(Unsuccessful_login),
        Set(varAttempts, varAttempts + 1);
        Notify("Incorrect password. Attempt " & varAttempts + 1 & "
of 3.", NotificationType.Error);
        Navigate(Unsuccessful_login)
    ),
    "Receptionist",
    If(
        varAttempts >= 2,
        Set(varIsBlocked, true);
        Notify("You have been blocked after 3 unsuccessful
attempts.", NotificationType.Error);
        Patch(
            IncorrectLogins,
            Defaults(IncorrectLogins),
            {
                UserName: TextInput1.Text,
                CreatedOn: Now()
            }
        );
        Navigate(Unsuccessful_login),
        Set(varAttempts, varAttempts + 1);
        Notify("Incorrect password. Attempt " & varAttempts + 1 & "
of 3.", NotificationType.Error);
        Navigate(Unsuccessful_login)
    ),
    "Pharmacist",
    If(
        varAttempts >= 2,
        Set(varIsBlocked, true);
        Notify("You have been blocked after 3 unsuccessful
attempts.", NotificationType.Error);
        Patch(
            IncorrectLogins,
            Defaults(IncorrectLogins),
            {
                UserName: TextInput1.Text,

```

```
                CreatedOn: Now()
            }
        );
        Navigate(Unsuccessful_login),
        Set(varAttempts, varAttempts + 1);
        Notify("Incorrect password. Attempt " & varAttempts + 1 & "
of 3.", NotificationType.Error);
        Navigate(Unsuccessful_login)
    ),
    Notify("Incorrect username or password.", NotificationType.Error)
// Default case for roles not found
    )
)
);

// Reset the input fields
Reset(TextInput1);
Reset(TextInput2);
```