**CCT College Dublin**

**Assessment Cover Page**

|  |  |
| --- | --- |
| **Module Title:** | Time and Task Management |
| **Assessment Title:** | Formation of an IT Consultancy company |
| **Lecturer Name:** | James Garza |
| **Student Full Name:** | Chukwudera Eden Ugochukwu, Pedro Silles, Jefferson Ramos |
| **Student Number:** | 2023285, 2023248, 2023240 |
| **Assessment Due Date:** | 22nd October |
| **Date of Submission:** | 2nd October |

**Declaration ;**

|  |
| --- |
| By submitting this assessment, I confirm that I have read the CCT policy on Academic Misconduct and understand the implications of submitting work that is not my own or does not appropriately reference material taken from a third party or other source. I declare it to be my own work and that all material from third parties has been appropriately referenced. I further confirm that this work has not previously been submitted for assessment by myself or someone else in CCT College Dublin or any other higher education institution. |

Table of Contents

[COVER PAGE 2](#_Toc148872679)

[INTRODUCTION 3](#_Toc148872680)

[**COMPANY DEPARTMENTS** 3](#_Toc148872681)

[THE MANAGEMENT DEPARTMENT 3](#_Toc148872682)

[SALES & MARKETING DEPARTMENT 3](#_Toc148872683)

[RESEARCH AND DEVELOPMENT 3](#_Toc148872684)

[COMPANY’S CULTURE 4](#_Toc148872685)

[SECURITY AWARENESS TRAINING 5](#_Toc148872686)

[PLANNING PROCESS 6](#_Toc148872687)

[**FIRST WEEK** 6](#_Toc148872688)

[**SECOND WEEK** 6](#_Toc148872689)

[**THIRD WEEK** 7](#_Toc148872690)

[DEVELOPING PROCESS 8](#_Toc148872691)

[REFERENCE LIST 9](#_Toc148872692)

# COVER PAGE

A close-up of a logo

Description automatically generated

# **INTRODUCTION**

When starting a company in this time and age its essential to computerize most, if not all operations within the company. That’s where JPC Defence comes in. JPC Defence is a cybersecurity firm aimed at providing small start-ups with affordable and quality digital security. Giving these start-ups the opportunity to expand their operations at a faster rate without worrying about data being stolen or corrupted.

We provide training session for staff to ensure they don’t expose the company to third party risk.

## **COMPANY DEPARTMENTS**

JPC Defence is divided into 3 departments to efficiently run day-to-day operations. These departments are listed below with the head of each department.

* Management Department – Chukwudera Eden Ugochukwu
* Sales & Marketing – Pedro Silles
* Research and Development - Jefferson Ramos

Each department works hand in hand in order to provide maximum satisfaction to our clients. A brief summary of the duty of each department is given below:

### THE MANAGEMENT DEPARTMENT

At the most fundamental level, management is a discipline that consists of a set of five general functions: planning, organizing, staffing, leading and controlling (Davis, 2019). In general the management team is in charge of maintaining and improving the relationship between the client and the firm. Consultation periods, operation methods and recruiting is all decided and followed up by the management department. This departments aim is to provide our clients with organized programmes and activities to fulfil their needs.

### SALES & MARKETING DEPARTMENT

Sales and marketing departments are the face of a company, engaging with customers, managing sensitive data, and leveraging technology platforms (Roohparvar, 2023). This department’s main focus is to create a social media Prescence for the company. Attracting clients through various means and spreading information regarding the operations of the firm are among the basic duties of those in this department.

### RESEARCH AND DEVELOPMENT

The research and development department is in charge of finding new ways to effectively help our clients. whether it’s by discovering new methods to protect data, or finding more effective software to aid with data protection, this department always strives to find new and effective ways to completely satisfy our clients.

# **COMPANY’S CULTURE**

Our culture is mostly based on transparency, and every member of our team is committed to client pleasure. Since JPD’s main goal is to help the newly created companies, we’re ready to provide them with the best explanations available, emphasising the minimum details, as they all need to know where they’re at and where they can reach working with us.

Additionally, our team is composed of young adults who have experience enough to handle any situation they might face in the future. A friendly and exciting team is what makes our environment work smoothly and consequently gives us better results. There’s no secret; once everything works, everyone can follow whichever way they find better.

Finally, it’s all about security. As a cyber security company, our mission is not only to provide clients with the best safety on their websites but also to show them that our team is ready to provide them with every sort of feedback and punctuality needed. We want them to feel safe, even after their shifts.

# **SECURITY AWARENESS TRAINING**

Our first project is based on training small and medium companies to ensure that their employees and collaborators will be able to reduce the risk of human error such as clicking on malicious links or falling for phishing scams. We are going to divide the training into 4 topics: personal devices, passwords, phishing attacks and suspicious URLs.

1. Personal devices: We are going to demonstrate to them how to choose and install an Anti-virus software based on their need, role and level of risk.
2. Passwords: How to build a good and strong password, pointing out the bad things to avoid and reduce risk. The use of password managers, software able to generate complex passwords for all accounts.
3. Phishing attacks: How to avoid having sensitive information leaked such as passwords, usernames, bank account information, credit cards, etc. Ways most used for attackers to reach people can also be conducted by text message, social media, email, or phone. The collaborator will be able to identify and report suspicious phishing attempts (IT Governance, 2016).
4. Suspicious URLs: How to identify and avoid malicious websites and links, based on the most recent technology and improvement of AI. Showing study of cases and sophisticated approaches from cybercriminals.
5. Social engineering: Identifying the behaviour and approach of social engineers to manipulate, influence and coerce people, in order to access internal data or steal sensitive information.
6. Data leakage: Consequences and types of data leakage, how to procedure in case of damage and corrupt databases. Prevention tools, to help the team to avoid accidental exposure and identify suspicious intentional breaches. Note that only in Ireland the number of personal data breaches from 25 May 2018 to 27 January 2023 was 29.692 (Petrosyan, A. 2023).

# **PLANNING PROCESS**

Our planning process did not take time to sort. On the first day as a group, we decided deadlines and first tasks to be done.

We successfully completed every task by the following weekend, and then we began working on the successive tasks the next week. What helped us a lot in deciding those tasks was breaking them down into smaller activities; it made the process easier.

One thing we needed to be careful about was the task dependencies, once we had in mind that the entire process would be interconnected. Due to our excellent communication, it went through smoothly.

In the end, our plan was to put every document made and uploaded to GitHub by each of us together and just adjust some points that we assumed we could adjust -nothing much. After doing that, we were done.

## **FIRST WEEK**

Company’s name, vision, logo and department selection was decided and done by the following weekend, no issues.

A screenshot of a computer

Description automatically generated

## **SECOND WEEK**

With the essential made, it was time to start the structure, introduction and first project. This phase demanded more time and attention than the first one, but we managed to have them done by Sunday again.

A screenshot of a computer

Description automatically generated

## **THIRD WEEK**

Finally, the last bunch. We had no issue going through them, done by Saturday night to have it submitted by Sunday afternoon.

A screenshot of a computer

Description automatically generated

# **DEVELOPING PROCESS**

The company goal was based on the needs of the market. After some research, it was clear that there is a gap in the cyber security market. The development of new technologies and the improvement of AI brought an increased number of scams and data leakage, which has demonstrated how unprepared people are when it comes to keeping their security on the internet and their own computers. Consequently, it was realized that those people must be trained and able to maintain a good and secure use of the internet and their devices.

Training people about cyber security was the solution found to solve the leakage of data and to fill the market gap. For this reason, it was developed the first project named “Security Awareness Training Program” which is divided into six modules: personal devices, passwords, phishing attacks, suspicious URLs, social engineering and data leakage.

The election of the manager was decided by a voting process. Firstly, all members had five minutes each to explain why they should be chosen and how they would deal with conflicts and people management. Eden Ugochukwu was elected due to demonstrated leadership skills and persuasive discourse. Pedro Silles mentioned his background in sales and market which matched with the needs of the project. Jefferson Ramos came up with some ideas of what the project could be in his speech, and what was linked with research and development.

Every step and decision made was thinking about how people could be allocated for each part of the project and agreed upon by all members of the group.

# **REFERENCE LIST**

* Davis, B. (2019). *Principles of Great Management*. [online] The University of Arizona Global Campus. Available at: https://www.uagc.edu/blog/5-principles-of-great-management#:~:text=At%20the%20most%20fundamental%20level.
* Roohparvar, R. (2023). *The Importance of Cybersecurity for Sales and Marketing Departments*. [online] Cyber Security Solutions, Compliance, and Consulting Services - IT Security. Available at: https://www.infoguardsecurity.com/the-importance-of-cybersecurity-for-sales-and-marketing-departments/ [Accessed 19 Oct. 2023].
* IT Governance (2016). *What is phishing? Everything you need to know | IT Governance UK*. [online] Itgovernance.co.uk. Available at: <https://www.itgovernance.co.uk/phishing>.
* Petrosyan, A. (2023). *Number of personal data breaches in Europe 2022*. [online] Statista. Available at: <https://www.statista.com/statistics/1203667/total-personal-data-breaches-europe/#:~:text=Since%20the%20General%20Data%20Protection>