# *IT Security (420-F30-HR)*

# *Assignment 3 – Business*

Date assigned: Tuesday, April 15 (Friday schedule)

Date due: Friday, May 20, 23h50

Tuesday, April 29, 1pm, Milestone 1

**Learning Objectives**

Upon successful completion of this assignment, the student will:

1. Analyze a use case and make recommendations
2. Create security policy recommendations for a business
3. Create access control recommendations for a business
4. Create a professional report

To do:

# Part A – Use Case

Analyze the use case specified in Appendix A. Review the associated rubric to this assignment.

If it’s not detailed in the Use case, assume the worst case. State all your assumptions that drive any of your decisions.

Generally, if there’s an item you need to know, ask in the class’ MS Teams channel for this assignment.

You have been asked to analyze the business and complete a report for the IT manager who graduated from Heritage College in 2017, way before IT security was taught.

The goal of your report is to analyze the current business practices and propose new business practices to improve their IT security.

Resources: course material

[NIST Cybersecurity Framework 2.0 Small Business Quick-Start Guide](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf).

Ask if there’s any further resources you need.

# Report

You must provide context relevant to your audience.

The general format of the report is:

1. Cover page
2. Table of Contents
3. Introduction
   1. Purpose
   2. Target Audience
4. Body
   1. NIST CSF 2.0 – what is it and the process we’re going to follow
   2. Govern
   3. Identify
   4. Protect
   5. Detect
   6. Respond
   7. Recover
   8. Analysis – where have the following principles been applied in your best practice recommendations? A chart/matrix/table is a good way to summarize this.
      1. Least Privilege
      2. Least common mechanism
      3. Defense in Depth
5. Conclusion – summary of benefits once best practices are followed

Throughout the document you must make sure that the following is covered:

1. Security Policies
   1. What are they and why they’re important
2. IT Security Best Practices/Policies
   1. For each best practice, ensure you cover:
      1. What’s done in the organization now and possible risks.
      2. Explain the best practice (what is it, why it’s done)
      3. Proposed application of the best practice to the organization. Your proposal for this policy.
   2. Best practices to cover:
      1. Physical Security
      2. Employee Security – hiring, onboarding, and termination
      3. Employee access and awareness (acceptable use) – Web, Social networks, network use
      4. Data Security and Access Control – protecting the company data.
         1. IAAA model – define and specifically apply against company data/operations
         2. Analyze the data used and generated by the different departments. Provide a role-based access control identifying roles, operations and assets/object.
      5. Email Security – what email practices should employees follow
      6. Passwords
      7. Web & Hosting security – network, devices and server setup. Provide a network diagram
      8. Compliance – Privacy laws, customer rights
      9. Monitoring and Periodic checks

This report is fully self-contained. i.e. assume the reader only has what you provide (and not this assignment or any other course material). You are playing the role of an IT security expert addressing a client who does not have an IT Security background.

This will be written following the Technical writing guidelines based on the Google Technical Writing Style guide that you learnt in Advanced Topics I.

# Milestones

|  |  |  |
| --- | --- | --- |
| 1 | April 29 before class | Report outline– cover page, complete Intro, body (skeleton is sectioned out – 1-2 sentences of context per section/subsection explaining to the reader the purpose and value of the section (This is the **final content** you plan on presenting to the reader, and not a draft. The intent is to show a clear understanding of your organization), Conclusion (skeleton), confirm rubric has been read and understood.  If you have a section/sub-section header, have 1-2 sentences for context for the reader. |
| 2 | May 9, 23h50 | Asset categories and RBAC model complete. Items for milestone 2 are clearly marked in the rubric (M2) |

You will be provided a minimum of 90 minutes of lab time to work on the assignment (more *may* be provided).

# Rubric

See external spreadsheet on Moodle.

Take a look at the rubric to ensure you understand how this assignment will be assessed.

# To submit

When you have completed the assignment, upload: **YourUserName\_A03\_F30\_Report.docx** to MS Teams.

# Appendix A – Business Use Case

“Sam & Ella Gourmet Food” is an online company that ships a wide variety of gourmet specialty foods like smoked salmon, chocolates, and cheeses.

Diagram, circle

Description automatically generated

It is a relatively new company, that started out in the private kitchens of partners Ella and Sam and rapidly grew to a company of over 65 employees in the span of two years.

Customers are primarily from Canada, and the European Union. The online store accepts transactions in Canadian dollars and Euros.

The company supports single orders, but most customers enjoy monthly subscriptions, like “Cheese of the Month”.

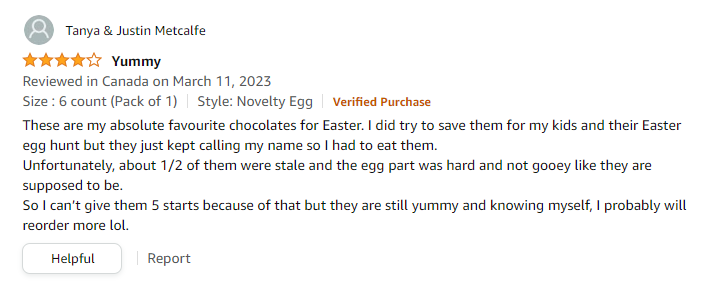
Despite being an online store (there is no “brick & mortar” storefront), Ella and Sam have had little experience in building an online presence and built the IT quickly under very chaotic conditions.

**Customers**

On customer registration, the company collects User’s name, email address, shipping address, phone number, credit card, date of birth, religion, ethnicity, photo, food likes/dislikes, billing information and allergy information. On their birthday month, subscription customers get a complementary chocolate gift bundle and a nice, personalized card.

Customer registration to the site is simple, simply asking for the user information and confirming the email address is valid.

Subscription customers are encouraged to rate the items in their monthly bundle so that the company can improve customization of the monthly packages and marketing material. Customers enjoy reading the comments and ratings left behind by other customers.



Every month, marketing material is customized and emailed to each customer based on matching algorithms on what they might like most. The customer will get suggestions on things they might like and see how it was rated by other customers, past and present, showing their rating feedback (comments, names, dates ).

The proprietary matching algorithm on what to ship each customer is a function of what the customer is known to have liked, what the customer is likely to like (new things to try), and things the company is over stocked in (it is a business, after all).

There are currently 2100 customers. On average, 42 customers leave per month, 87 new customers sign up per month. When a customer leaves, their account credentials are disabled so that they can’t log in again.

Customers can register and edit their account profile information via the web site.

**Employees and Organization**

Departments are:

* Help desk / Customer support
* Development team (Web apps and data-mining algorithms)
* Shipping & Logistics
* Production & Manufacturing
* Finance & Accounting
* Marketing
* IT

Each department has a manager that reports to company owners, Ella and Sam.

The whole company is located in a large warehouse in Gatineau, Quebec, which has 3 floors :

* Offices and desks on the top 2 floors with open concept seating. There’s no closed offices, but break out rooms are provided for meetings.
* Operations such as storage, production and shipping take place on the ground floor

A picture containing text, indoor, floor, ceiling

Description automatically generated

The company has an employee lounge and eating area on the 3rd floor where free drinks are provided, and free samples of the company products. Tacos are delivered on Tuesdays. The staff go into a frenzy when they see the taco delivery guy walks pasts their desks, heading up to the lounge and it’s a great communal/social event.

**IT**

There is a single web application used internally by all departments, with specific menu options used by each department.

All data and menu options are accessible to employees once logged on.

The web application and database are currently running on the server located in an equipment closet near the IT department’s office space.

A different web application is used for the customer facing web site though both applications access the same back-end database.

There is a single server hosting all the server functions (DB, web server, applications, etc.) connected to the internal network. The server is used by all the departments to run their operations. Each server function (DB, web server, applications, etc.) has it’s own local username/password management.

Diagram

Description automatically generated

**Data**

Each type of user consumes and generates data.

Here is a sample of what data is at the organization (it is incomplete)

|  |  |  |
| --- | --- | --- |
|  | Produces/Updates | Consumes |
| Help desk / Customer support | Trouble tickets | Customer Profile  Trouble tickets |
| Development team (Web apps and data-mining algorithms) | Source code  Test data  Data mining reports | Trouble Tickets |
| Shipping & Logistics | Shipping bills  Inventory tracking | Inventory (raw and produced)  Invoices |
| Production & Manufacturing | Inventory (raw and produced)  Inventory tracking | Invoice summaries |
| Finance & Accounting | Invoices  Employee Payroll | Employee Payroll |
| Marketing | Catalog/items  Newsletters/emails | Data mining reports |
| IT | Trouble Tickets | Trouble Tickets |
| Customer | Item comments/rankings  Orders (become Invoices) | Catalog |