Requirements for Compliance

Please complete the requirements on or before October 31, 2020

1. DATA REGISTRY

- Declaring your Operational Data Processes
As a personal information controller (the Club) or personal information processor (Employee), an organization must implement

reasonable and appropriate physical, technical and organizational measures for the protection of personal data.

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against

natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent

misuse, unlawful destruction, alteration, and contamination. This section gives you a general description of those measures.

Conduct a Departmental Privacy Impact Assessment (DPIA)

Example:

All department shall conduct a Privacy Impact Assessment (PIA) relative to all **activities**, **Operational procedures**,

projects and **systems** involving the processing of personal or confidential data.

Duty of Confidentiality

Example:

All employees will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate

and hold personal data under strict confidentiality if the same is not intended for public disclosure.

2. PROCESS REQUEST

Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.
Example:

There shall be a detailed and accurate documentation of all activities, projects and processing systems of the Club, to

be carried out by the Risk Management Officer, in coordination with the Data Protection Officer.

3. DATA SECURITY AWARENESS

Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security
Example:

The Club shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved

in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as

often as necessary.

4. 5S CHECKLIST

This portion shall feature the procedures intended to monitor and limit access to the facility containing the personal data,

including the activities therein. It shall provide for the actual design of the facility, the physical arrangement

of equipment and furniture and the schedule and means of retention and disposal of data, among others. To ensure that mechanical

destruction, tampering and alteration of personal data under the custody of the Club are protected from

man-made disasters, power disturbances, external access, and other similar threats, provisions like the following must be included

in the 5S Checklist:

1. **Format of data to be collected**

Example:

Personal data in the custody of the Clubs Department may be in digital/electronic format and paper-based/physical format.

2. Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/ separate room or part of an existing room);

Example:

All personal and confidential data being processed by the department shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the MIS with encryption.

3. Access procedure of the Clubs personnel

Example:

Only authorized personnel shall be allowed inside the data room or confidential area. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitation of access to room or facility

Example:

All personnel authorized to enter and access the data room or facility must fill out and register with the online registration platform of the organization, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration, and purpose of each access.

5. Design of office space/work station

Example:

The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6. Persons involved in processing, and their duties and responsibilities

Example:

Persons involved in processing shall always maintain confidentiality and integrity of

personal data. They are not allowed to bring their own gadgets or storage device of any

form when entering their offices or station

7. Modes of transfer of personal data within the organization, or to third parties

Example:

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data,

including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal or

confidential data.

8. Retention and disposal procedure

Example:

The organization shall retain the personal data of a client for one (1) year from the data

of purchase. Upon expiration of such period, all physical and electronic copies of the

personal data shall be destroyed and disposed of using secure technology.

5. DATA INVENTORY

A data inventory is a fully described record of the data assets maintained by the Clubs department. The inventory

records basic information about a data asset including its name, contents, update frequency, use license, owner/maintainer,

privacy considerations, data source, and other relevant details.

Why Conduct an Inventory?

Managing a data inventory reduces risk and uncertainty by creating a checklist for security and compliance requirements

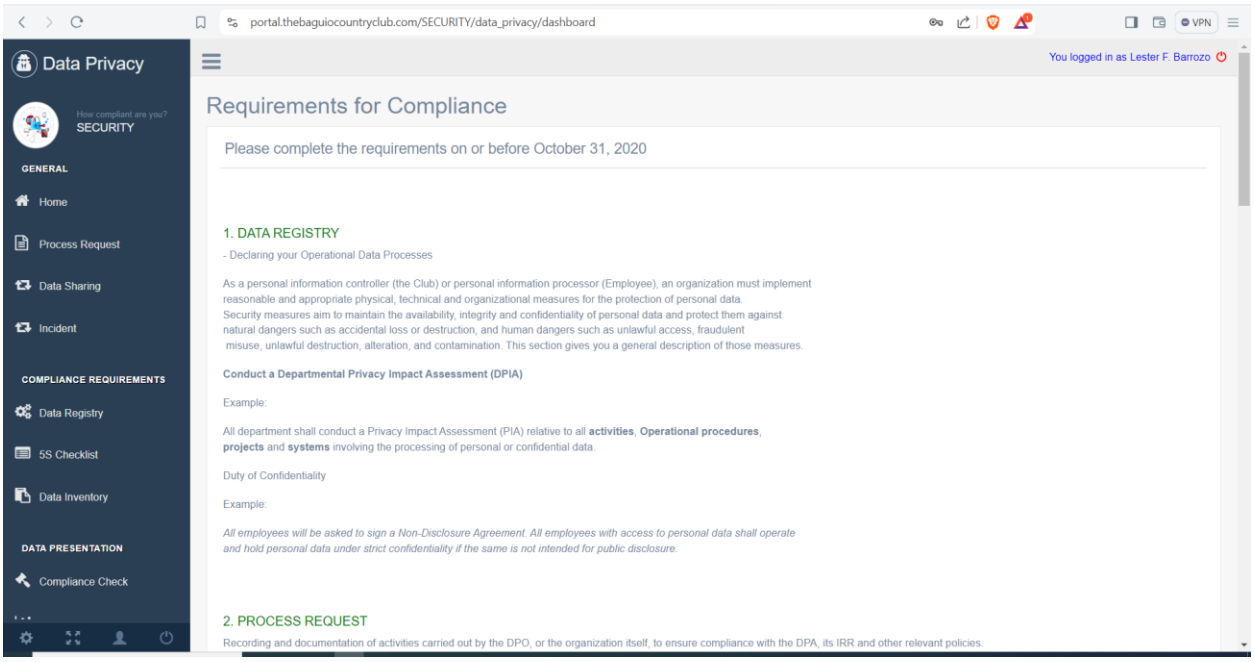
and improves a city’s ability to designate accountability for the quality of the data collected and created.

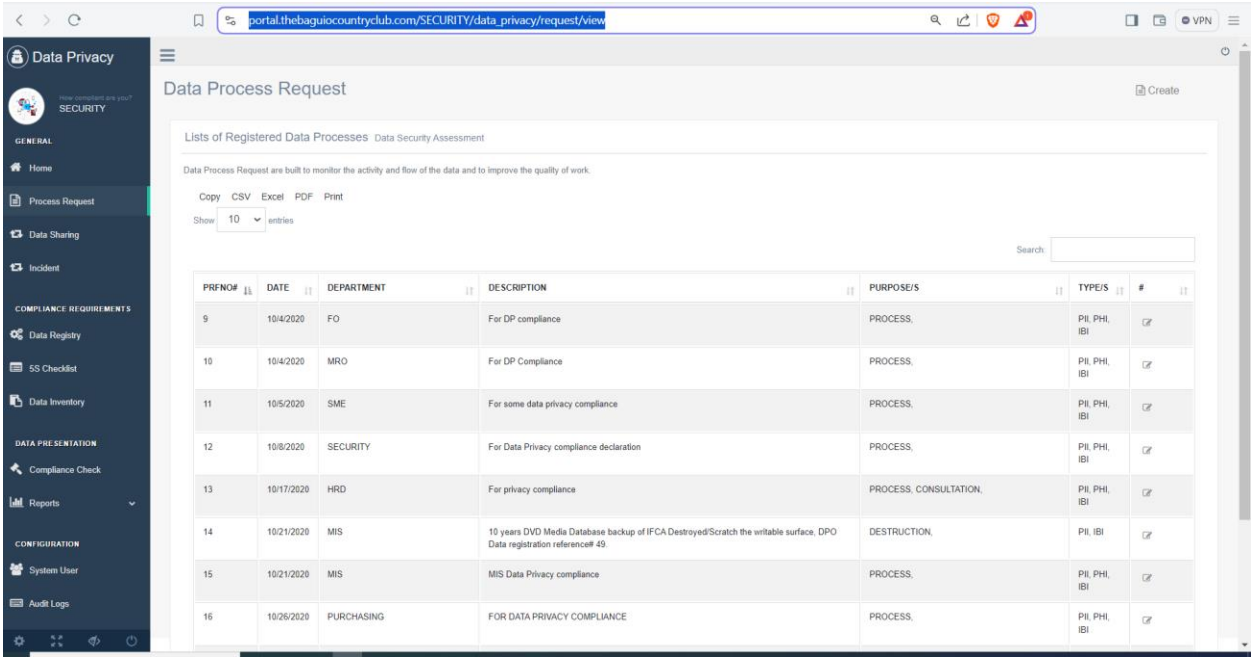
Example:

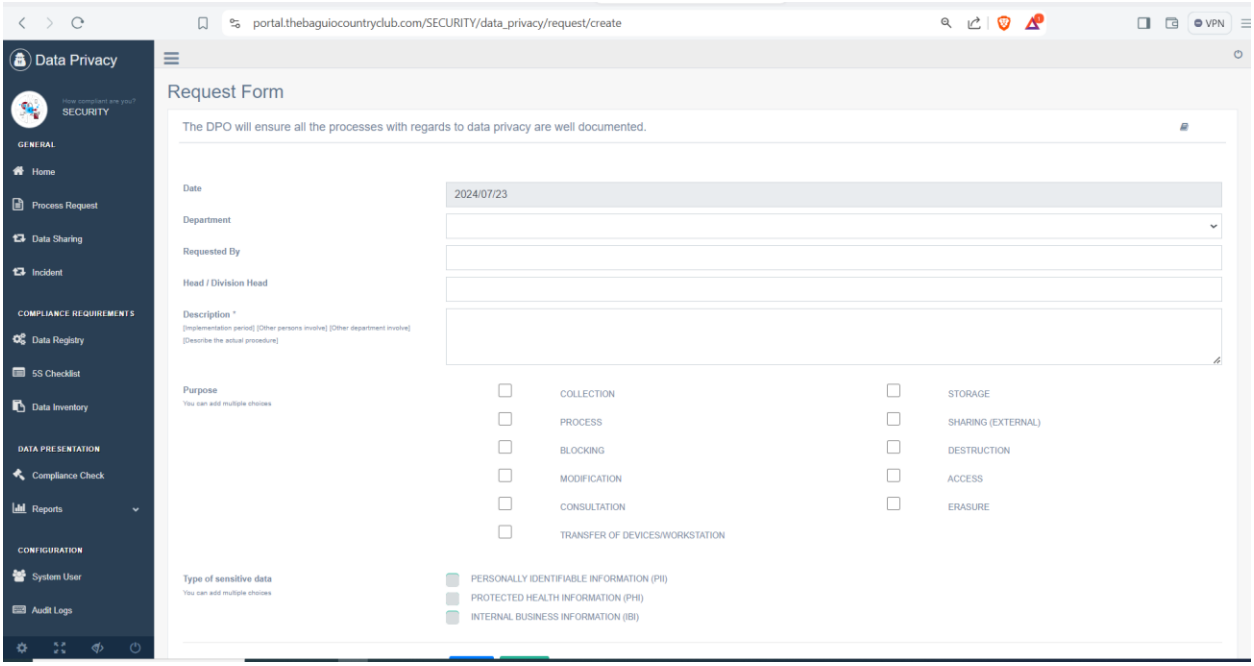
The datasets worth inventorying are those which are considered assets to employees, departments, executive

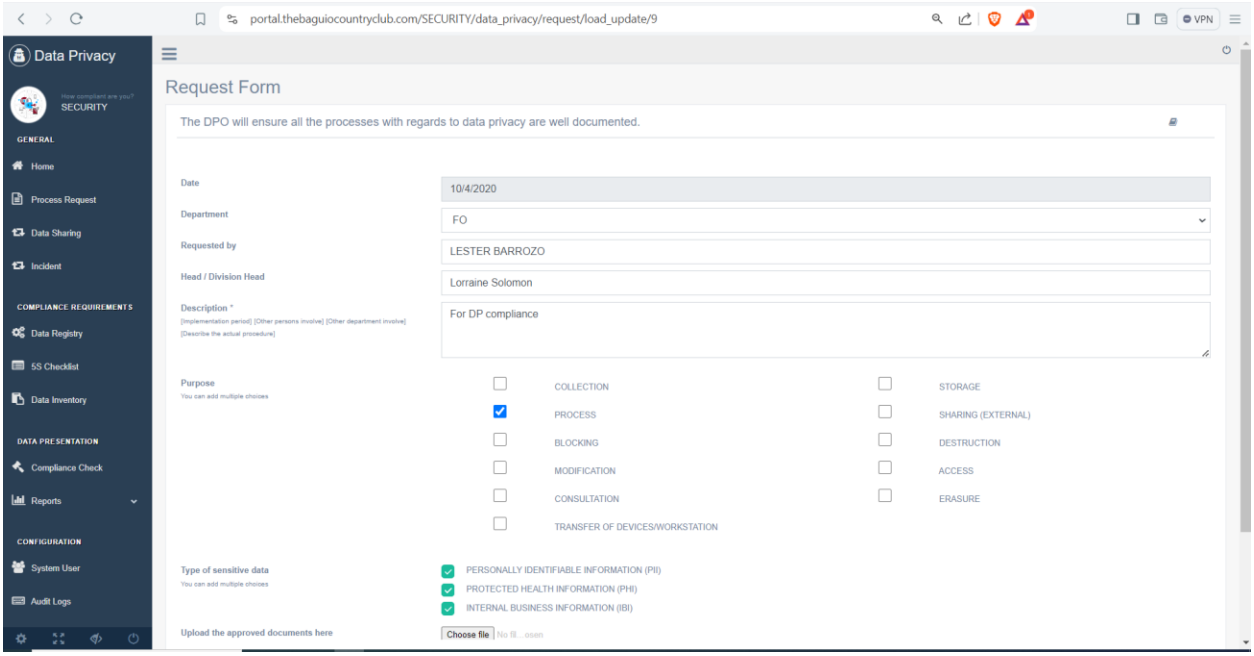
leadership, and the general public. Data assets can range from individual datasets that are connected to forms

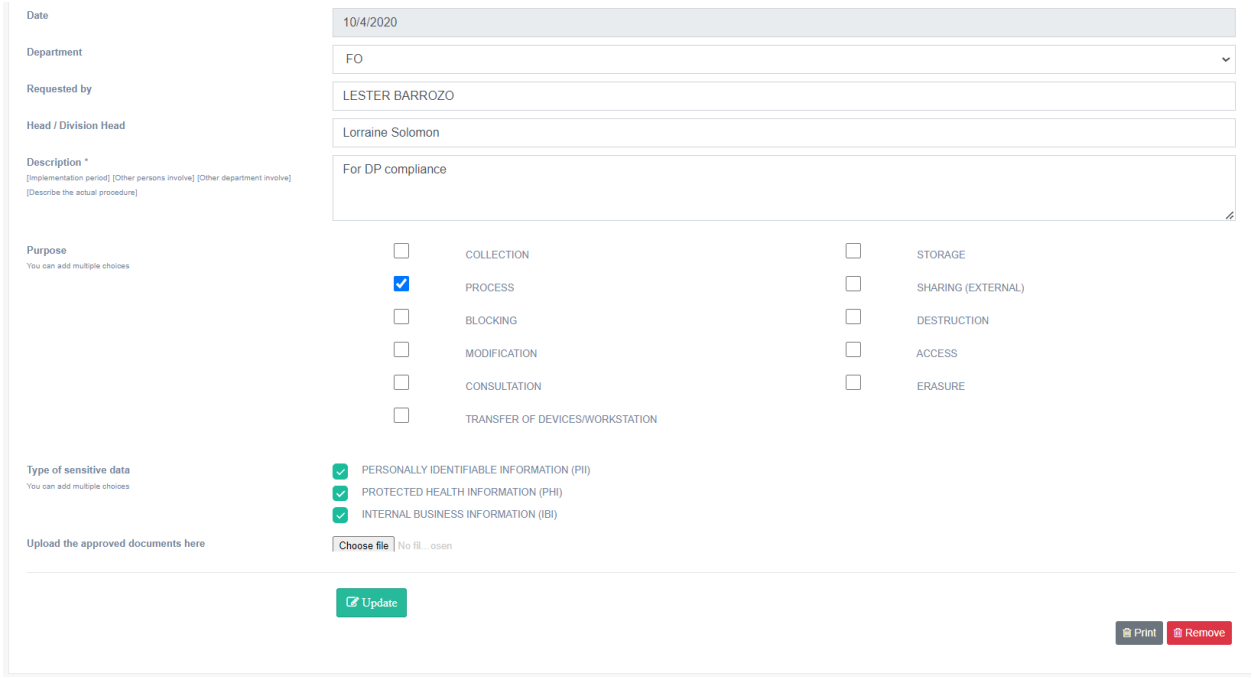
that people fill out, to integrated databases that track a city's operations.

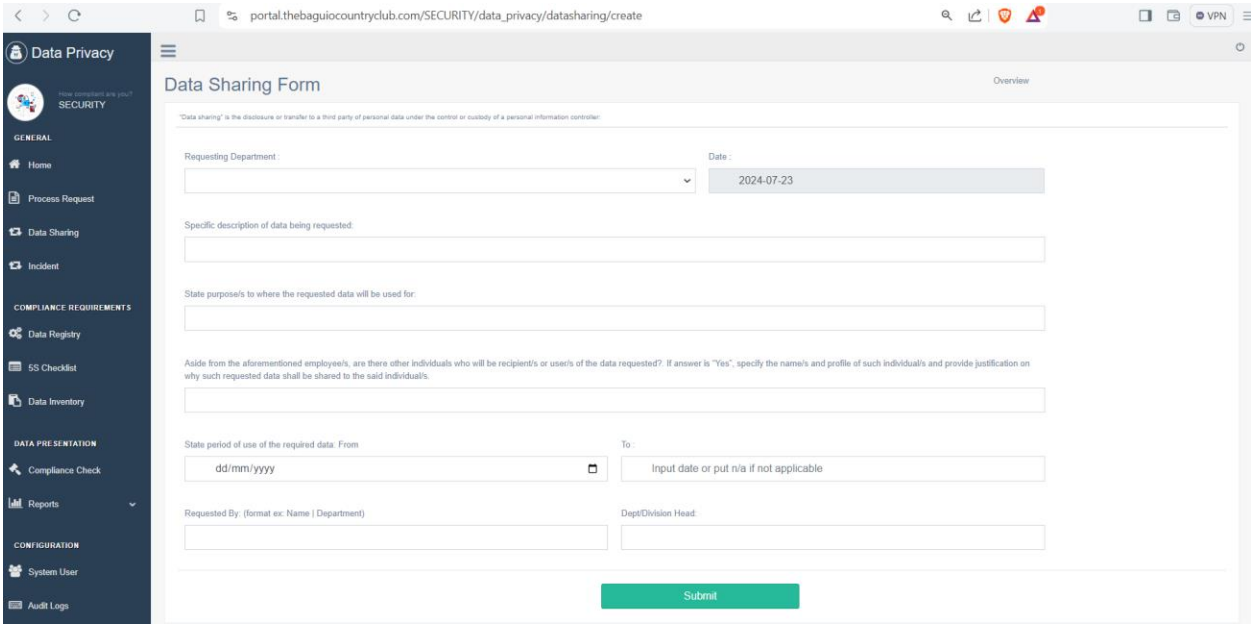


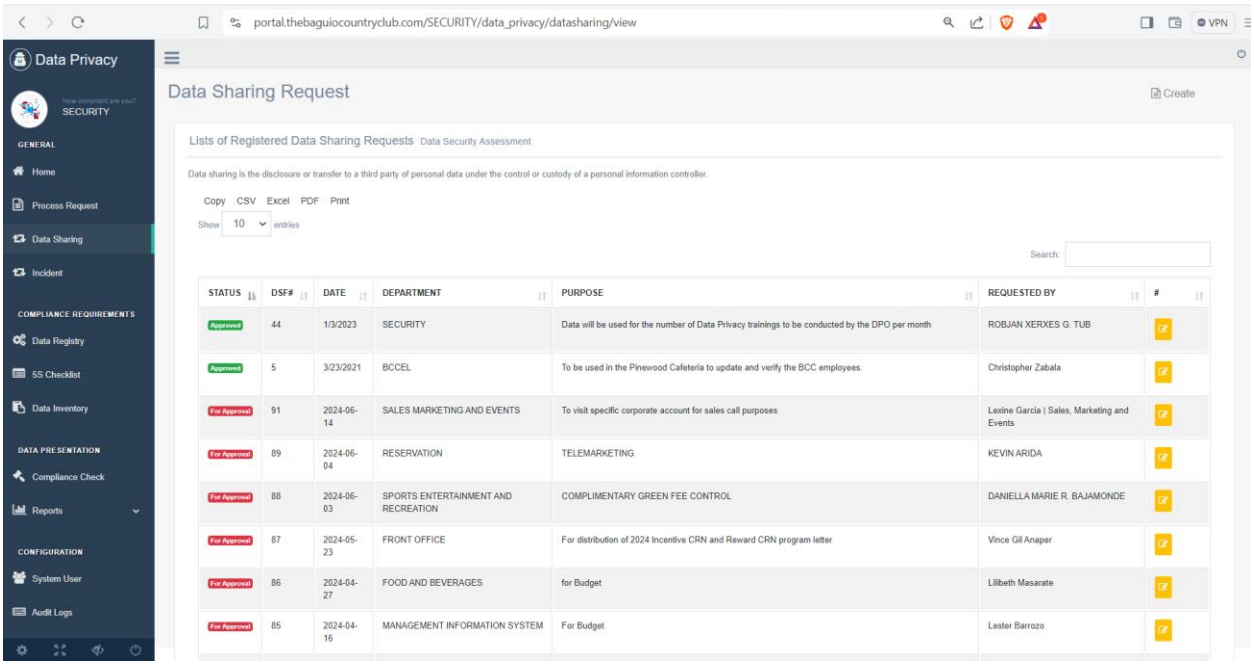


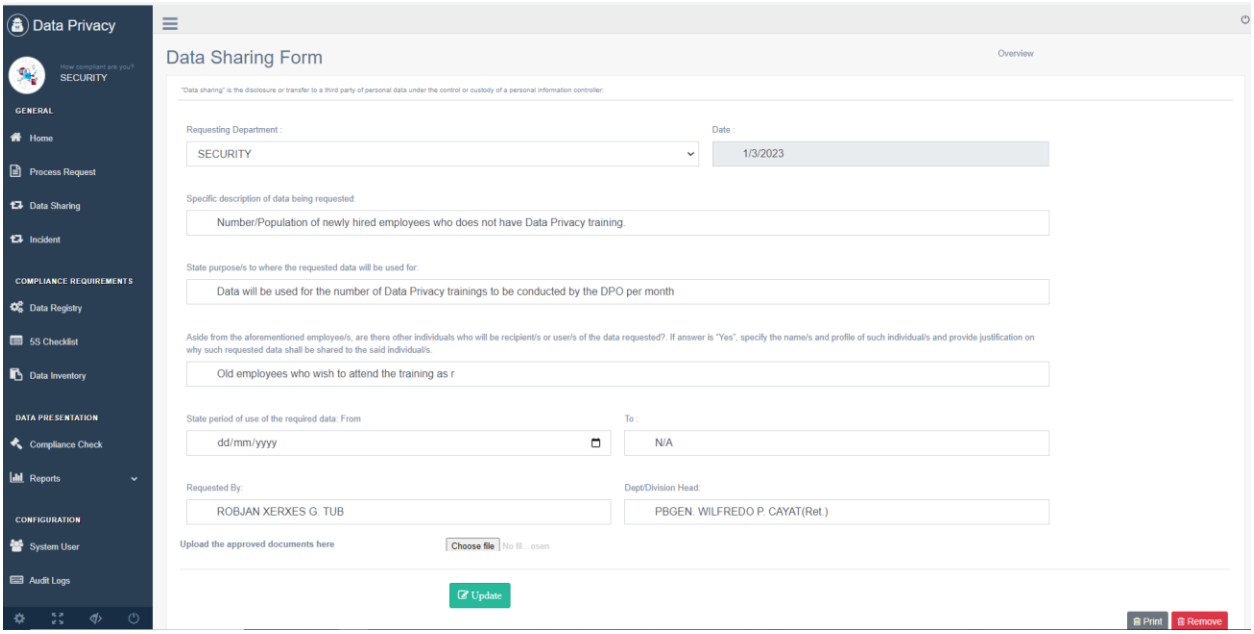

portal.thebaguiocountryclub.com/SECURITY/data_privacy/request/create
Data Privacy
How compliant are you?
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Request Form
The DPO will ensure all the processes with regards to data privacy are well documented.
Date
2024/07/23
Department
Requested By
Head / Division Head
Description *
[Implementation period] [Other persons involve] [Other department involve]
[Describe the actual procedure]
Purpose
You can add multiple choices
COLLECTION
STORAGE
PROCESS
SHARING (EXTERNAL)
BLOCKING
DESTRUCTION
MODIFICATION
ACCESS
CONSULTATION
ERASURE
TRANSFER OF DEVICES/WORKSTATION
Type of sensitive data
You can add multiple choices
PERSONALLY IDENTIFIABLE INFORMATION (PII)
PROTECTED HEALTH INFORMATION (PHI)
INTERNAL BUSINESS INFORMATION (IBI)

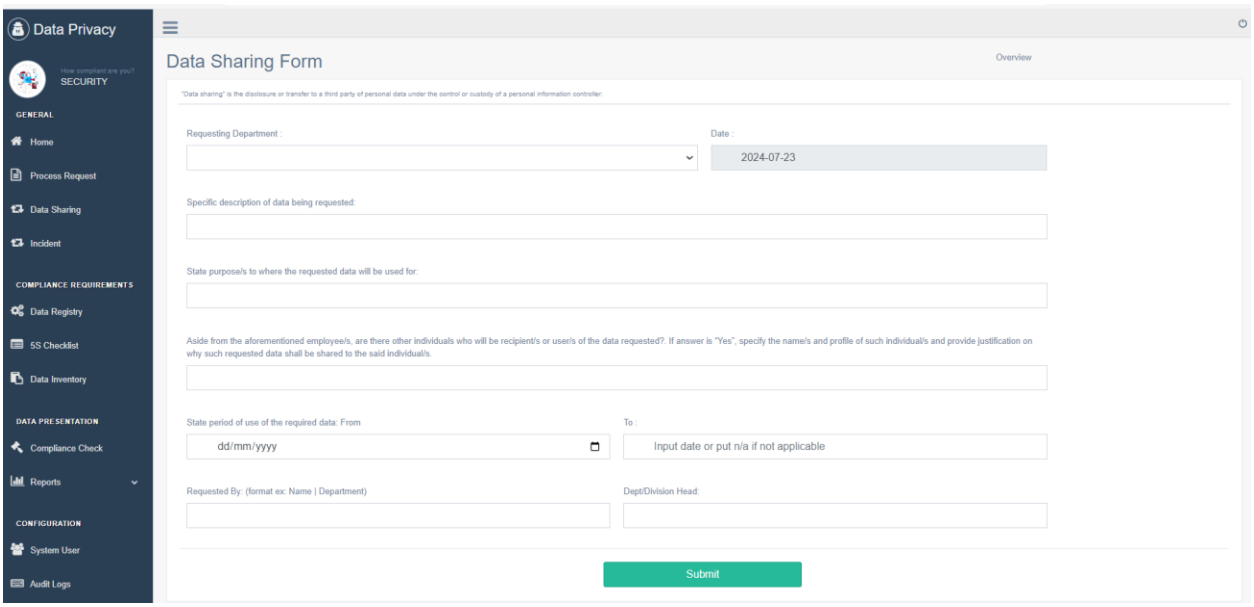

portal.thebaguiocountryclub.com/SECURITY/data_privacy/request/load_update/9
Data Privacy
How compliant are you?
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Request Form
The DPO will ensure all the processes with regards to data privacy are well documented.
Date
10/4/2020
Department
FO
Requested by
LESTER BARROZO
Head / Division Head
Lorraine Solomon
Description *
[Implementation period] [Other persons involve] [Other department involve]
[Describe the actual procedure]
For DP compliance
Purpose
You can add multiple choices
COLLECTION
STORAGE
PROCESS
SHARING (EXTERNAL)
BLOCKING
DESTRUCTION
MODIFICATION
ACCESS
CONSULTATION
ERASURE
TRANSFER OF DEVICES/WORKSTATION
Type of sensitive data
You can add multiple choices
PERSONALLY IDENTIFIABLE INFORMATION (PII)
PROTECTED HEALTH INFORMATION (PHI)
INTERNAL BUSINESS INFORMATION (IBI)
Upload the approved documents here
Choose file

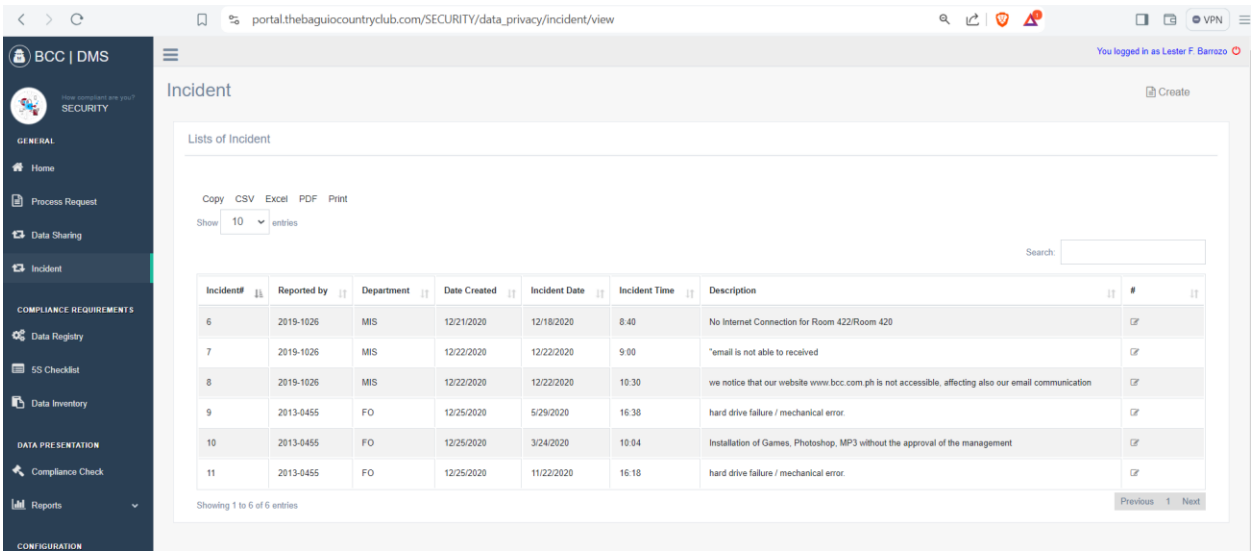

Date
10/4/2020
Department
FO
Requested by
LESTER BARROZO
Head / Division Head
Lorraine Solomon
Description *
[Implementation period] [Other persons involve] [Other department involve] [Describe the actual procedure]
For DP compliance
Purpose
You can add multiple choices
COLLECTION
PROCESS
BLOCKING
MODIFICATION
CONSULTATION
TRANSFER OF DEVICES/WORKSTATION
STORAGE
SHARING (EXTERNAL)
DESTRUCTION
ACCESS
ERASURE
Type of sensitive data
You can add multiple choices
PERSONALLY IDENTIFIABLE INFORMATION (PII)
PROTECTED HEALTH INFORMATION (PHI)
INTERNAL BUSINESS INFORMATION (IBI)
Upload the approved documents here
Choose file
No fil...osen
Update
Print
Remove

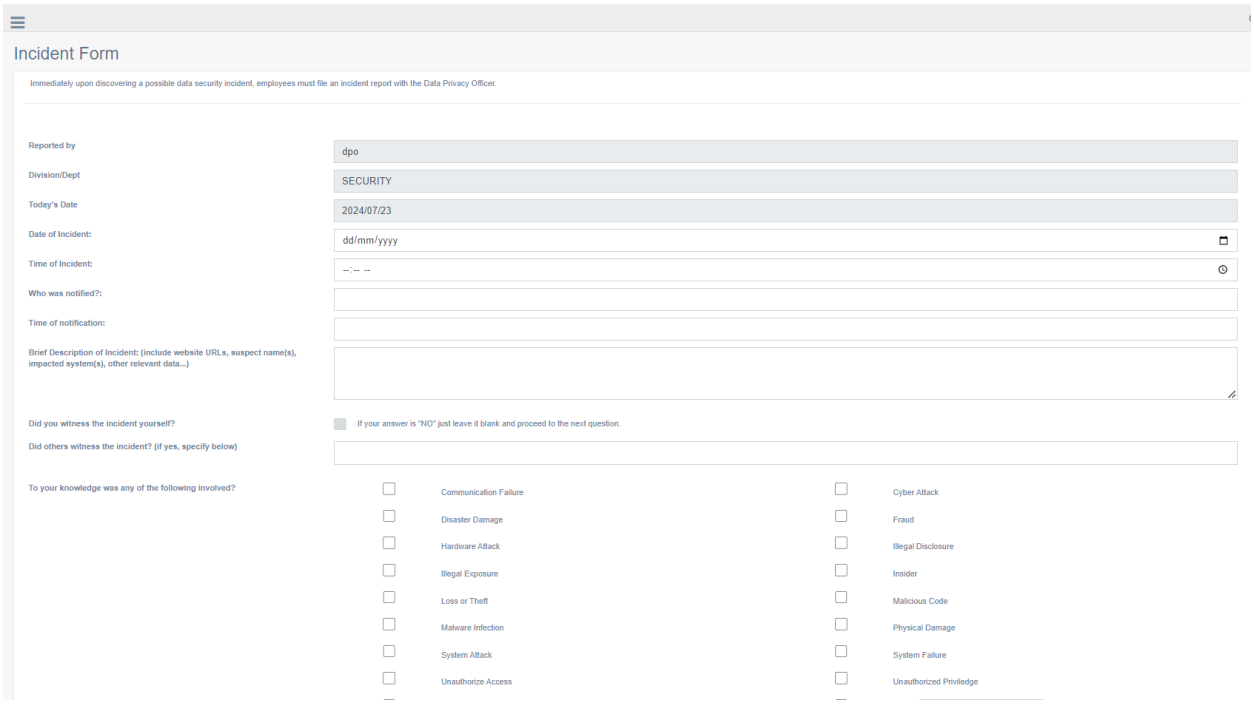

portal.thebaguiocountryclub.com/SECURITY/data_privacy/datasharing/create
VPN
Data Privacy
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Data Sharing Form
Overview
"Data sharing" is the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.
Requesting Department :
Date :
2024-07-23
Specific description of data being requested:
State purpose/s to where the requested data will be used for:
Aside from the aforementioned employee/s, are there other individuals who will be recipient/s or user/s of the data requested?. If answer is "Yes", specify the name/s and profile of such individual/s and provide justification on why such requested data shall be shared to the said individual/s.
State period of use of the required data: From
dd/mm/yyyy
To :
Input date or put n/a if not applicable
Requested By: (format ex: Name | Department)
Dept/Division Head:
Submit


portal.thebaguiocountryclub.com/SECURITY/data_privacy/datasharing/view
Data Privacy
How compliant are you? SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Data Sharing Request
Create
Lists of Registered Data Sharing Requests Data Security Assessment
Data sharing is the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.
Copy CSV Excel PDF Print
Show 10 entries
Search:
STATUS DSF# DATE DEPARTMENT PURPOSE REQUESTED BY #
Approved 44 1/3/2023 SECURITY Data will be used for the number of Data Privacy trainings to be conducted by the DPO per month ROBJAN XERXES G. TUB
Approved 5 3/23/2021 BCCEL To be used in the Pinewood Cafeteria to update and verify the BCC employees. Christopher Zabala
For Approval 91 2024-06-14 SALES MARKETING AND EVENTS To visit specific corporate account for sales call purposes Lexine Garcia | Sales, Marketing and Events
For Approval 89 2024-06-04 RESERVATION TELEMARKETING KEVIN ARIDA
For Approval 88 2024-06-03 SPORTS ENTERTAINMENT AND RECREATION COMPLIMENTARY GREEN FEE CONTROL DANIELLA MARIE R. BAJAMONDE
For Approval 87 2024-05-23 FRONT OFFICE For distribution of 2024 Incentive CRN and Reward CRN program letter Vince Gil Anaper
For Approval 86 2024-04-27 FOOD AND BEVERAGES for Budget Lilibeth Masarate
For Approval 85 2024-04-16 MANAGEMENT INFORMATION SYSTEM For Budget Lester Barrozo

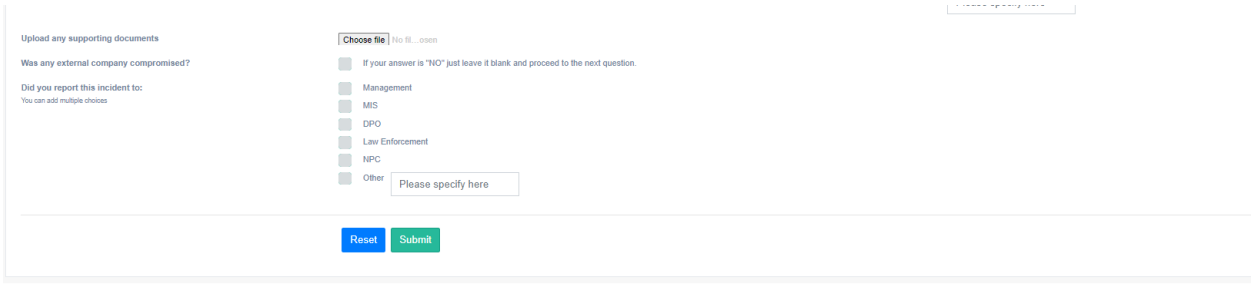

Data Privacy
How compliant are you? SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Data Sharing Form
Overview
"Data sharing" is the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.
Requesting Department :
SECURITY
Date :
1/3/2023
Specific description of data being requested:
Number/Population of newly hired employees who does not have Data Privacy training.
State purpose/s to where the requested data will be used for:
Data will be used for the number of Data Privacy trainings to be conducted by the DPO per month
Aside from the aforementioned employee/s, are there other individuals who will be recipient/s or user/s of the data requested?. If answer is "Yes", specify the name/s and profile of such individual/s and provide justification on why such requested data shall be shared to the said individual/s.
Old employees who wish to attend the training as r
State period of use of the required data: From
dd/mm/yyyy
To :
N/A
Requested By:
ROBJAN XERXES G. TUB
Dept/Division Head:
PBGEN. WILFREDO P. CAYAT(Ret.)
Upload the approved documents here
Choose file
Update
Print
Remove

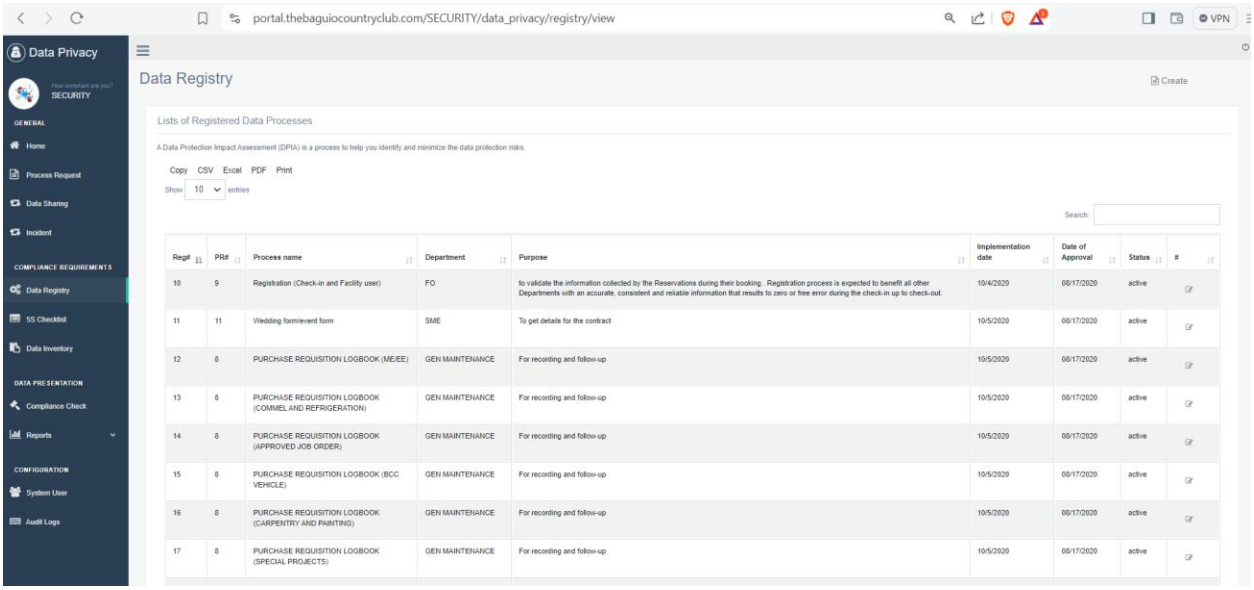

Data Privacy
How compliant are you? SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Data Sharing Form
Overview
"Data sharing" is the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.
Requesting Department :
Date :
2024-07-23
Specific description of data being requested:
State purpose/s to where the requested data will be used for:
Aside from the aforementioned employee/s, are there other individuals who will be recipient/s or user/s of the data requested? If answer is "Yes", specify the name/s and profile of such individual/s and provide justification on why such requested data shall be shared to the said individual/s.
State period of use of the required data: From
dd/mm/yyyy
To :
Input date or put n/a if not applicable
Requested By: (format ex: Name | Department)
Dept/Division Head:
Submit

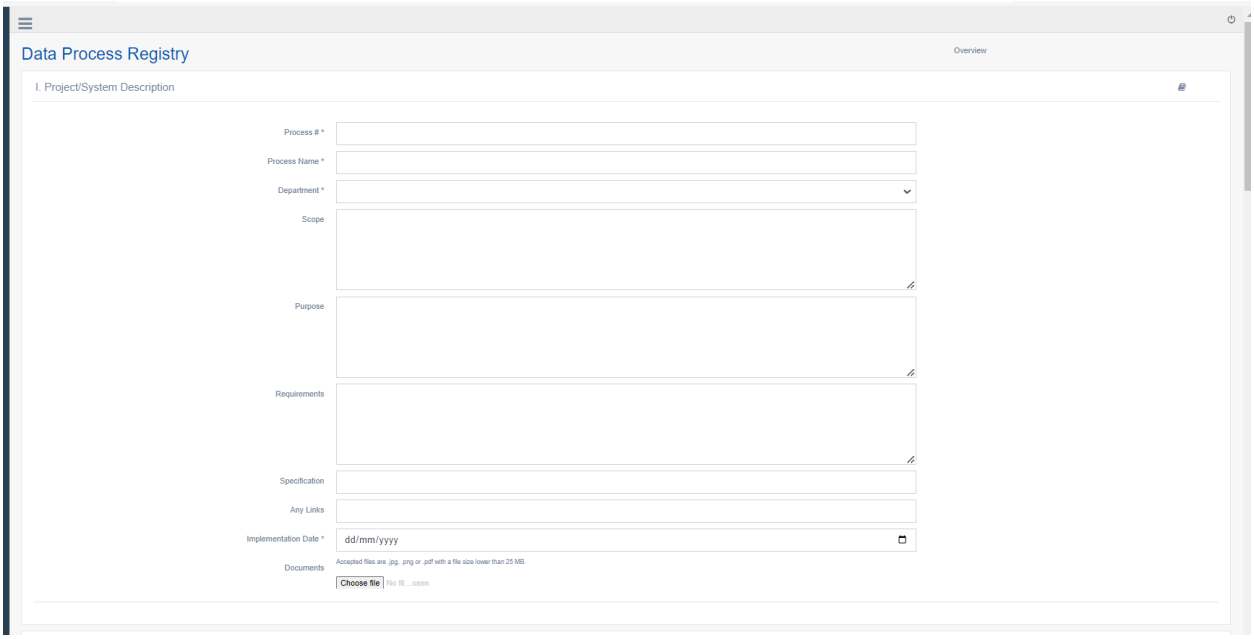

portal.thebaguiocountryclub.com/SECURITY/data_privacy/incident/view
VPN
BCC | DMS
You logged in as Lester F. Barrozo
How compliant are you? SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
Incident
Create
Lists of Incident
Copy CSV Excel PDF Print
Show 10 entries
Search:
Incident# Reported by Department Date Created Incident Date Incident Time Description #
6 2019-1026 MIS 12/21/2020 12/18/2020 8:40 No Internet Connection for Room 422/Room 420
7 2019-1026 MIS 12/22/2020 12/22/2020 9:00 "email is not able to received
8 2019-1026 MIS 12/22/2020 12/22/2020 10:30 we notice that our website www.bcc.com.ph is not accessible, affecting also our email communication
9 2013-0455 FO 12/25/2020 5/29/2020 16:38 hard drive failure / mechanical error.
10 2013-0455 FO 12/25/2020 3/24/2020 10:04 Installation of Games, Photoshop, MP3 without the approval of the management
11 2013-0455 FO 12/25/2020 11/22/2020 16:18 hard drive failure / mechanical error.
Showing 1 to 6 of 6 entries
Previous 1 Next

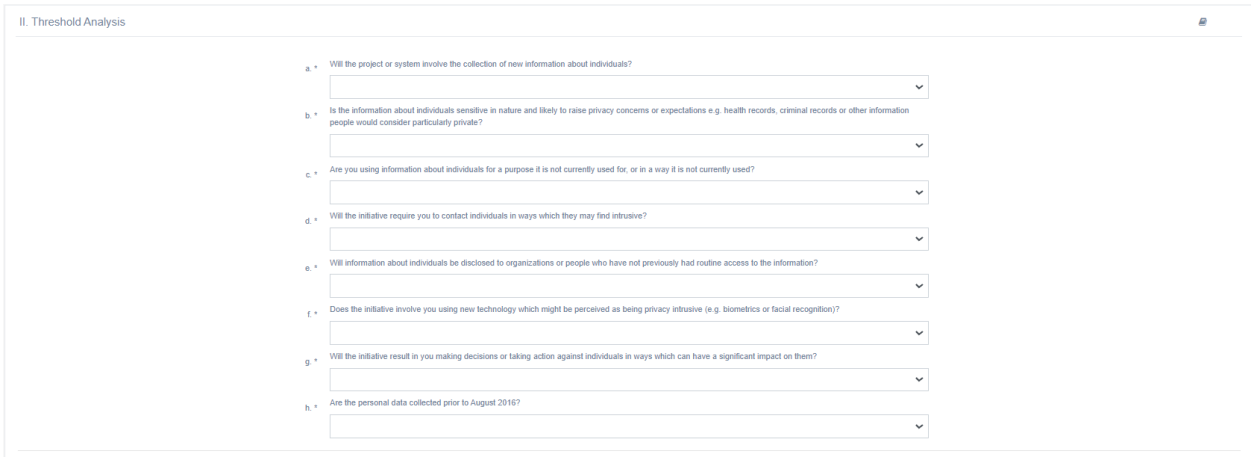

Incident Form
Immediately upon discovering a possible data security incident, employees must file an incident report with the Data Privacy Officer.
Reported by
dpo
Division/Dept
SECURITY
Today's Date
2024/07/23
Date of Incident:
dd/mm/yyyy
Time of Incident:
--:-- --
Who was notified?:
Time of notification:
Brief Description of Incident: (include website URLs, suspect name(s), impacted system(s), other relevant data...)
Did you witness the incident yourself?
If your answer is "NO" just leave it blank and proceed to the next question.
Did others witness the incident? (if yes, specify below)
To your knowledge was any of the following involved?
Communication Failure
Cyber Attack
Disaster Damage
Fraud
Hardware Attack
Illegal Disclosure
Illegal Exposure
Insider
Loss or Theft
Malicious Code
Malware Infection
Physical Damage
System Attack
System Failure
Unauthorize Access
Unauthorized Priviledge

:


Upload any supporting documents
Choose file
No fil...osen
Was any external company compromised?
If your answer is "NO" just leave it blank and proceed to the next question.
Did you report this incident to:
You can add multiple choices
Management
MIS
DPO
Law Enforcement
NPC
Other
Please specify here
Reset
Submit


portal.thebaguiocountryclub.com/SECURITY/data_privacy/registry/view
VPN
Data Privacy
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
Data Registry
Create
Lists of Registered Data Processes
A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimize the data protection risks.
Copy CSV Excel PDF Print
Show 10 entries
Search:
Reg# PR# Process name Department Purpose Implementation date Date of Approval Status #
10 9 Registration (Check-in and Facility user) FO to validate the information collected by the Reservations during their booking . Registration process is expected to benefit all other Departments with an accurate, consistent and reliable information that results to zero or free error during the check-in up to check-out. 10/4/2020 08/17/2020 active
11 11 Wedding form/event form SME To get details for the contract 10/5/2020 08/17/2020 active
12 8 PURCHASE REQUISITION LOGBOOK (ME/EE) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active
13 8 PURCHASE REQUISITION LOGBOOK (COMMEL AND REFRIGERATION) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active
14 8 PURCHASE REQUISITION LOGBOOK (APPROVED JOB ORDER) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active
15 8 PURCHASE REQUISITION LOGBOOK (BCC VEHICLE) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active
16 8 PURCHASE REQUISITION LOGBOOK (CARPENTRY AND PAINTING) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active
17 8 PURCHASE REQUISITION LOGBOOK (SPECIAL PROJECTS) GEN MAINTENANCE For recording and follow-up 10/5/2020 08/17/2020 active


Data Process Registry
Overview
I. Project/System Description
Process # *
Process Name *
Department *
Scope
Purpose
Requirements
Specification
Any Links
Implementation Date *
dd/mm/yyyy
Documents
Accepted files are .jpg, .png or .pdf with a file size lower than 25 MB.
Choose file
No fil...osen


II. Threshold Analysis
a. * Will the project or system involve the collection of new information about individuals?
b. * Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?
c. * Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
d. * Will the initiative require you to contact individuals in ways which they may find intrusive?
e. * Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?
f. * Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)?
g. * Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
h. * Are the personal data collected prior to August 2016?

III. Stakeholder(s) Engagement

* State all project stakeholders, consulted in conducting PIA. Identify which part they were involved. (Describe how stakeholders were engaged in the PIA process)

Name, Role, Involvement

IV. Personal Data Flows

* What personal data are being or will be processed by this project/system?

List all personal data (e.g. Personal Full Name, address, gender, phone number, etc.,) and state which is/ are the sensitive personal information (e.g. race, ethnicity, marital status, health, genetic, government issued numbers).

* Collection

1. State who collected or will be collecting the personal information and/or sensitive information.

2. How the personal information/sensitive personal information is collected and from whom it was collected?.

» If personal information is collected from some source other than the individual?

3. What is/are the purpose(s) of collecting the personal data?

» Be clear about the purpose of collecting the information
» Are you collecting what you only need?

4. How was or will the consent be obtained?

» Do individuals have the opportunity and/or right to decline to provide data?
» What happen if they decline?

4. How was or will the consent be obtained?

» Do individuals have the opportunity and/or right to decline to provide data?
» What happen if they decline?

* Storage

1. Where is it currently being stored?

» Is it being stored in a physical server or in the cloud?

2. Is it being stored in other country?

» If it is subject to a cross-border transfer, specify what country or countries.

3. Is the storage of data being outsourced?

» Specify if the storing process is being done in-house or is it handled by a service provider

* Usage

1. How will the data being used or what is the purpose of its processing?

» Describe how the collected information is being used or will be used
» Specify the processing activities where the personal information is being used.

* Retention

1. How long are the data being retained? And Why?

» State the length of period the data is being retained?
» What is the basis of retaining the data that long? Specify the reason(s)

2. The data is being retained by the organization or is it being outsourced?

» Specify if the data retention process is being done in-house or is it handled by a service provider

* Retention

1. How long are the data being retained? And Why?

» State the length of period the data is being retained?
» What is the basis of retaining the data that long? Specify the reason(s)

2. The data is being retained by the organization or is it being outsourced?

» Specify if the data retention process is being done in-house or is it handled by a service provider

* Disclosure/Sharing

1. To whom it is being disclosed to?

2. Is it being disclosed outside the organization? Why is it being disclosed?

» Specify if the personal information is being shared outside the organization
» What are the reasons for disclosing the personal information

* Disposal/Destruction

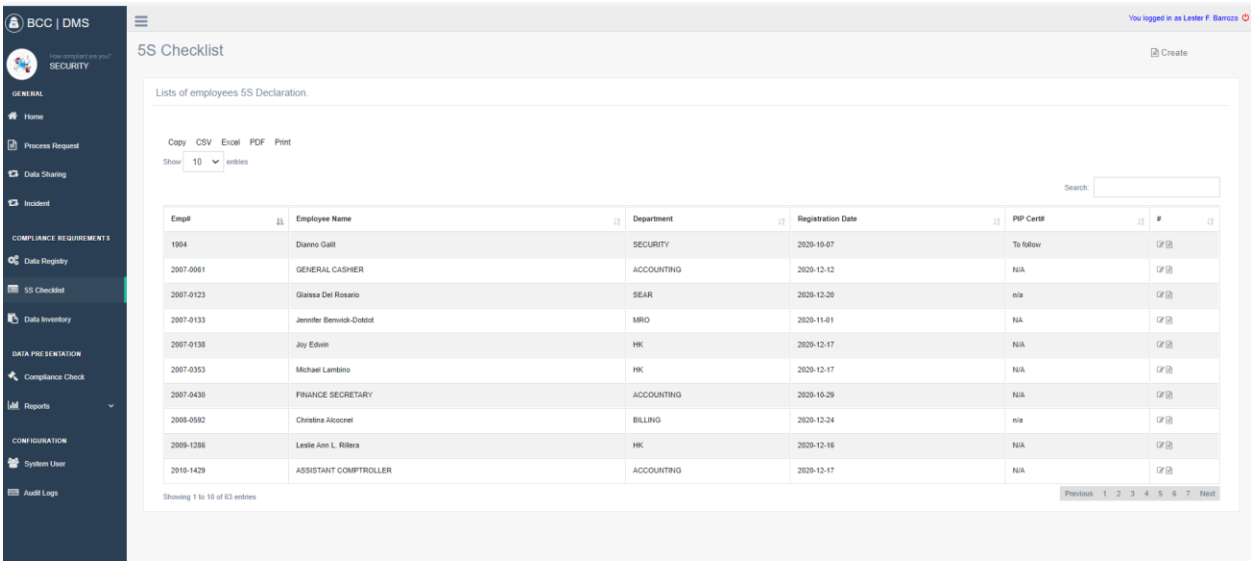
1. How will the data be disposed?

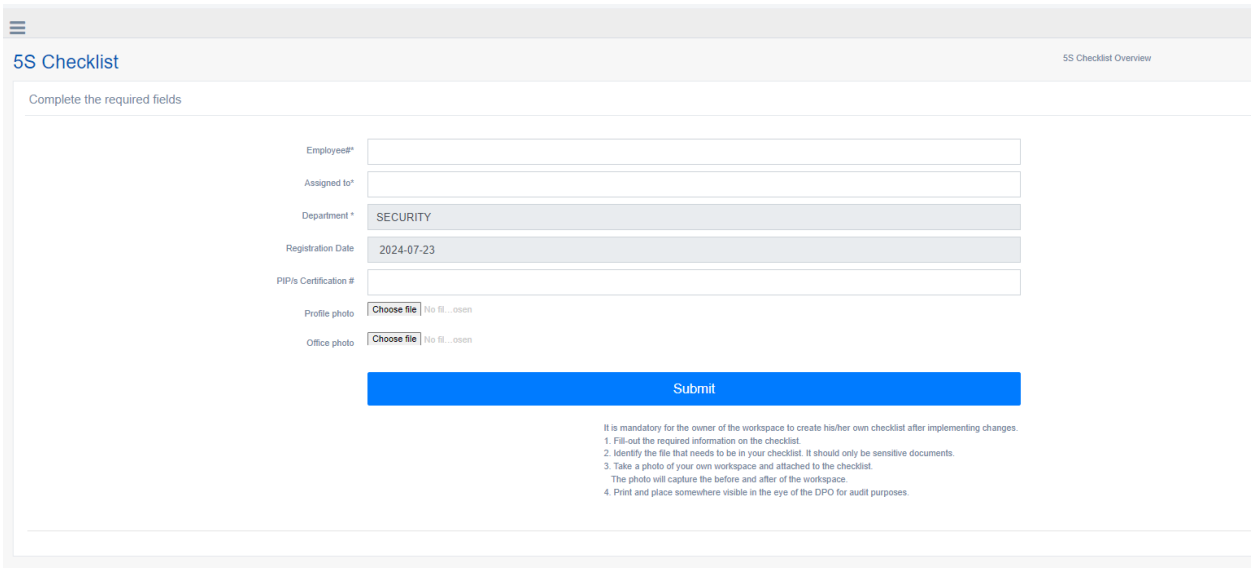
» Describe the process of disposing the personal information

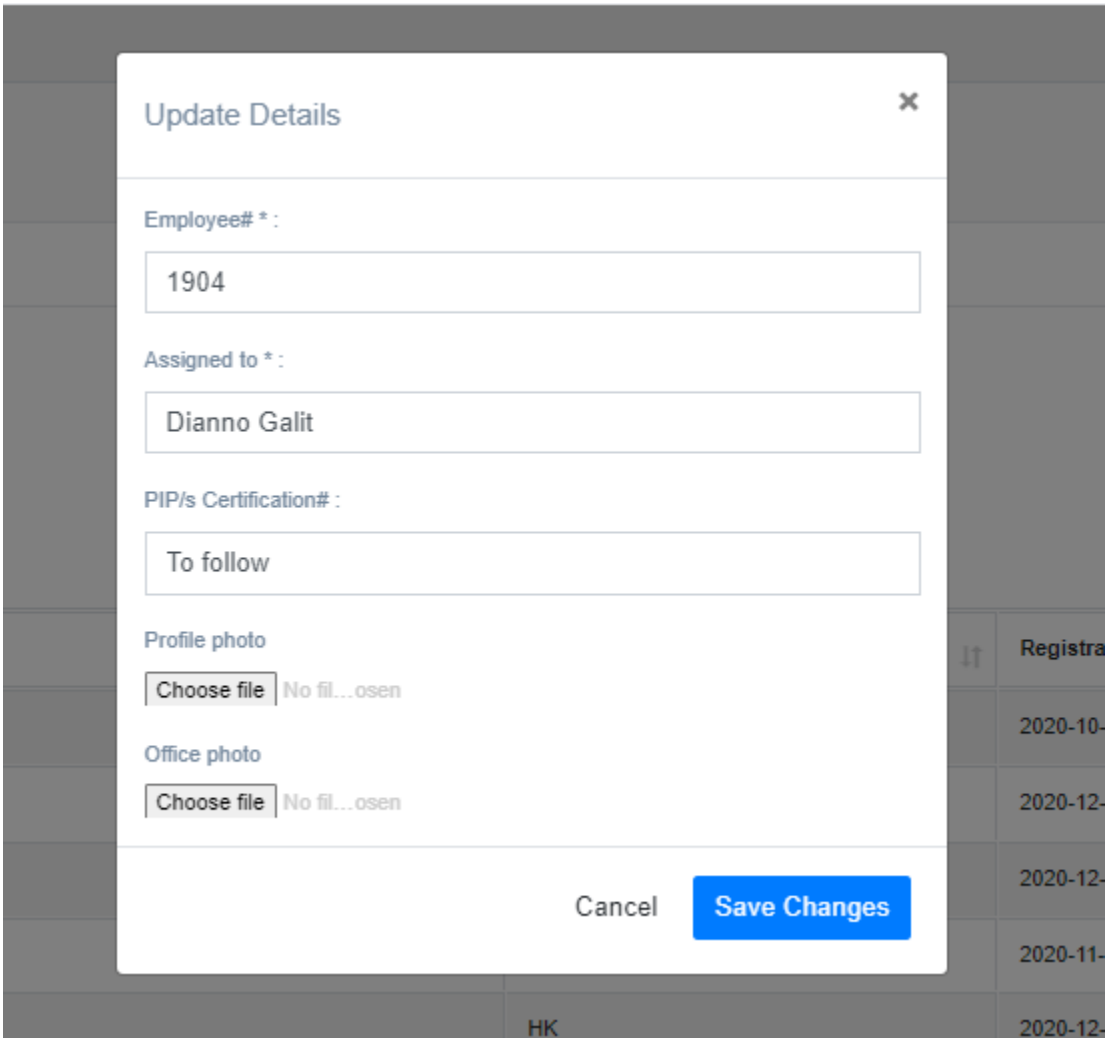
2. Who will facilitate the destruction of the data?

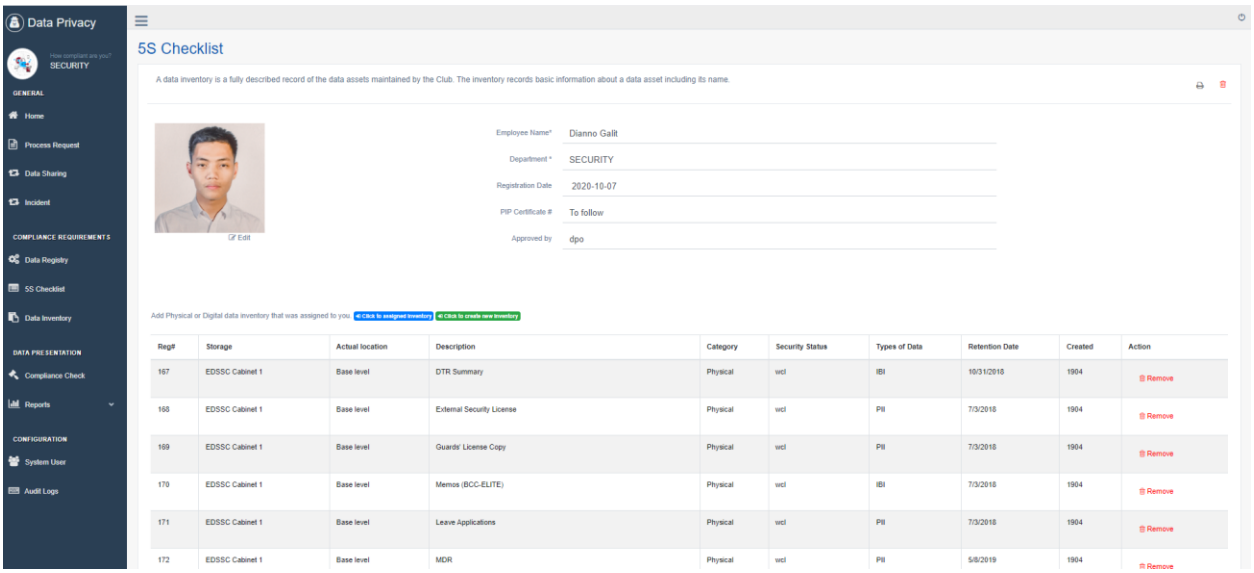
» State if the process is being managed in-house or if it is a third party

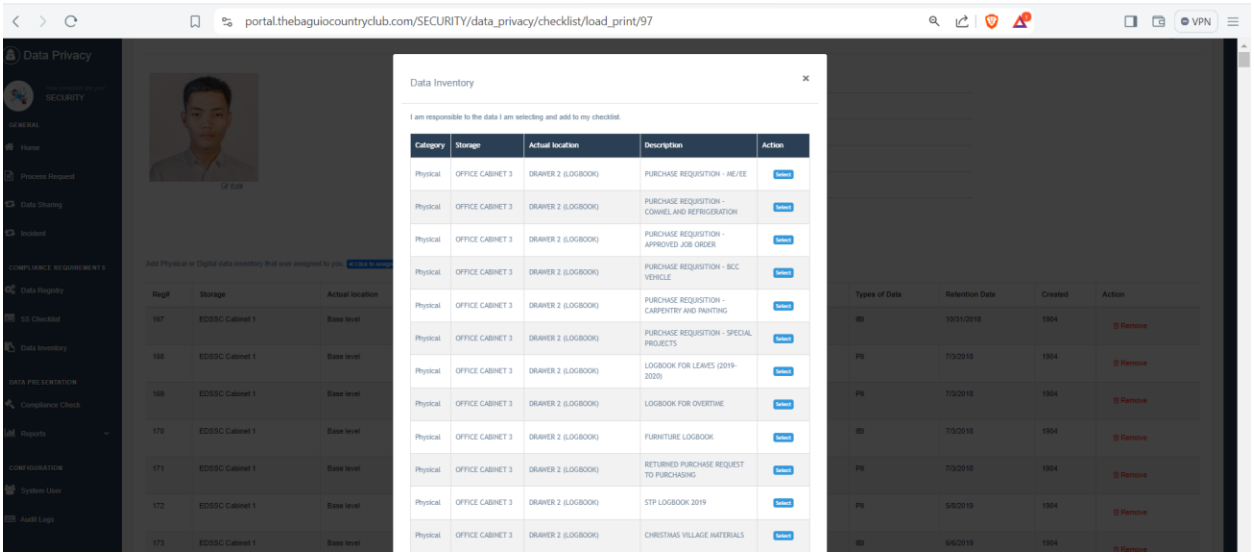
Submit

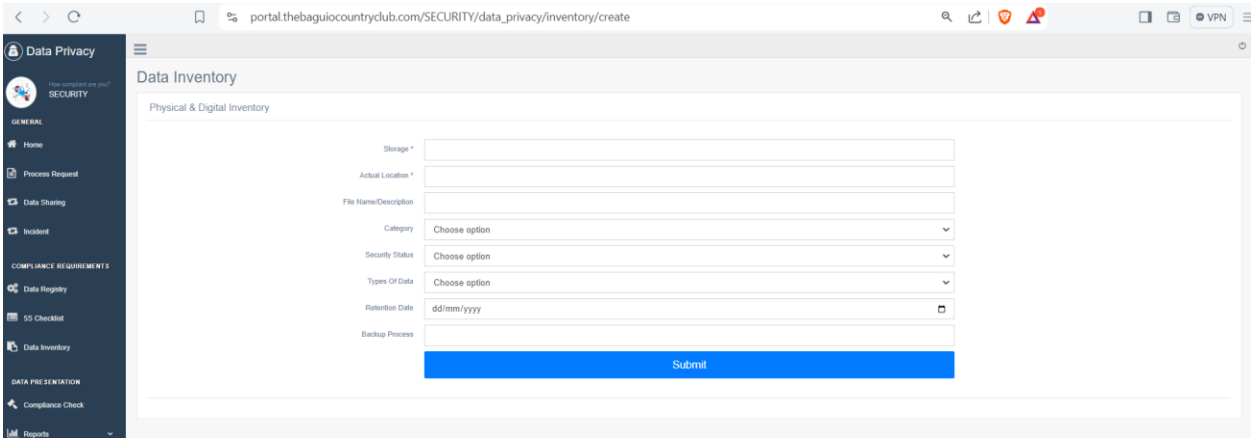



5S Checklist
5S Checklist Overview
Complete the required fields
Employee#*
Assigned to*
Department *
SECURITY
Registration Date
2024-07-23
PIP/s Certification #
Profile photo
Choose file
No fil...osen
Office photo
Choose file
No fil...osen
Submit
It is mandatory for the owner of the workspace to create his/her own checklist after implementing changes.
1. Fill-out the required information on the checklist.
2. Identify the file that needs to be in your checklist. It should only be sensitive documents.
3. Take a photo of your own workspace and attached to the checklist.
The photo will capture the before and after of the workspace.
4. Print and place somewhere visible in the eye of the DPO for audit purposes.


Update Details
Employee# * :
1904
Assigned to * :
Dianno Galit
PIP/s Certification# :
To follow
Profile photo
Choose file
No fil...osen
Office photo
Choose file
No fil...osen
Cancel
Save Changes
Registra
2020-10-
2020-12-
2020-12-
2020-11-
HK
2020-12-


Data Privacy
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
5S Checklist
A data inventory is a fully described record of the data assets maintained by the Club. The inventory records basic information about a data asset including its name.
Edit
Employee Name*
Dianno Galit
Department *
SECURITY
Registration Date
2020-10-07
PIP Certificate #
To follow
Approved by
dpo
Add Physical or Digital data inventory that was assigned to you.
Click to assigned inventory
Click to create new inventory
Reg# | Storage | Actual location | Description | Category | Security Status | Types of Data | Retention Date | Created | Action
167 | EDSSC Cabinet 1 | Base level | DTR Summary | Physical | wcl | IBI | 10/31/2018 | 1904 | Remove
168 | EDSSC Cabinet 1 | Base level | External Security License | Physical | wcl | PII | 7/3/2018 | 1904 | Remove
169 | EDSSC Cabinet 1 | Base level | Guards' License Copy | Physical | wcl | PII | 7/3/2018 | 1904 | Remove
170 | EDSSC Cabinet 1 | Base level | Memos (BCC-ELITE) | Physical | wcl | IBI | 7/3/2018 | 1904 | Remove
171 | EDSSC Cabinet 1 | Base level | Leave Applications | Physical | wcl | PII | 7/3/2018 | 1904 | Remove
172 | EDSSC Cabinet 1 | Base level | MDR | Physical | wcl | PII | 5/8/2019 | 1904 | Remove


portal.thebaguiocountryclub.com/SECURITY/data_privacy/checklist/load_print/97
VPN
Data Inventory
I am responsible to the data I am selecting and add to my checklist.
Category | Storage | Actual location | Description | Action
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - ME/EE | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - COMMEL AND REFRIGERATION | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - APPROVED JOB ORDER | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - BCC VEHICLE | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - CARPENTRY AND PAINTING | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | PURCHASE REQUISITION - SPECIAL PROJECTS | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | LOGBOOK FOR LEAVES (2019-2020) | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | LOGBOOK FOR OVERTIME | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | FURNITURE LOGBOOK | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | RETURNED PURCHASE REQUEST TO PURCHASING | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | STP LOGBOOK 2019 | Select
Physical | OFFICE CABINET 3 | DRAWER 2 (LOGBOOK) | CHRISTMAS VILLAGE MATERIALS | Select


portal.thebaguiocountryclub.com/SECURITY/data_privacy/inventory/create
VPN
Data Privacy
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
Data Inventory
Physical & Digital Inventory
Storage *
Actual Location *
File Name/Description
Category
Choose option
Security Status
Choose option
Types Of Data
Choose option
Retention Date
dd/mm/yyyy
Backup Process
Submit

5S Checklist

A data inventory is a fully described record of the data assets maintained by the Club. The inventory records basic information about a data asset including its name.

Edit

Employee Name* Dianno Galit

Department * SECURITY

Registration Date 2020-10-07

PIP Certificate # To follow

Approved by dpo

Lists of Physical and Digital data inventory that was assigned to you.

Reg#	Storage	Actual location	Description	Category	Security Status	Types of Data	Retention Date	Created
167	EDSSC Cabinet 1	Base level	DTR Summary	Physical	wcl	IBI	10/31/2018	1904
168	EDSSC Cabinet 1	Base level	External Security License	Physical	wcl	PII	7/3/2018	1904
169	EDSSC Cabinet 1	Base level	Guards' License Copy	Physical	wcl	PII	7/3/2018	1904
170	EDSSC Cabinet 1	Base level	Memos (BCC-ELITE)	Physical	wcl	IBI	7/3/2018	1904
171	EDSSC Cabinet 1	Base level	Leave Applications	Physical	wcl	PII	7/3/2018	1904
172	EDSSC Cabinet 1	Base level	MDR	Physical	wcl	PII	5/8/2019	1904
173	EDSSC Cabinet 1	Base level	Issued Radios for BCC Det.	Physical	wcl	IBI	6/6/2019	1904
174	EDSSC Cabinet 1	Base level	Order of Posting	Physical	wcl	PII	9/6/2018	1904
175	EDSSC Cabinet 1	Base level	Medical Certificate	Physical	wcl	PHI	7/1/2015	1904
176	EDSSC Cabinet 1	Base level	License to operate	Physical	wcl	IBI	11/9/2018	1904

BCC | DMS

SECURITY

GENERAL

Home

Process Request

Data Sharing

Incident

COMPLIANCE REQUIREMENTS

Data Registry

5S Checklist

Data Inventory

DATA PRESENTATION

Compliance Check

Reports

CONFIGURATION

System User

Audit Logs

You logged in as Lester F. Barrozo

Data Inventory

Create

Lists of current data inventory.

Copy CSV Excel PDF Print

Show 10 entries

Search:

Storage	Actual Location	File Description	Category	Security Stat	Dept	Data Types	Retention Date	Created	#
1 GREEN VAULT	ACCTG OFFICE	VAULT 9	Physical	wcl	ACCOUNTING	IBI	1/31/2025	2007-0430	
13 Steel Cabinets	Membership Record Room	Regular, Company, Special Courtesy, Young Professional, Local Resident, NBIRM, HLM, Reciprocal Clubs	Physical	wcl	MRO	PII	0001-01-01	2011-2137	
2 GREEN VAULTS	ACCTG OFFICE	VAULT 1-2	Physical	wcl	ACCOUNTING	IBI	1/1/2025	2007-0430	
2 GREEN VAULTS	ACCTG OFFICE	VAULT 3-4	Physical	wcl	ACCOUNTING	IBI	1/1/2025	2007-0061	
4 GREEN VAULTS	ACCTG OFFICE	VAULT 5-8	Physical	wcl	ACCOUNTING	IBI	1/31/2030	2007-0430	
8 Wooden Cabinets	Membership Record Room	Assorted Files	Physical	wcl	MRO	PII	0001-01-01	2011-2137	
Archiving Computer Table	Drawer 2	Logbook	Physical	wcl	SECURITY	IBI	0/0/0012	2017-0013	
Archiving Computer Table	Drawer 2	Coop and Archiving files	Physical	wcl	SECURITY	IBI	0/0/0013	2017-0014	
Assistant HR Manager's PC	Drive E	Local Disk C/ Asst. HR Manager/Competency Exams	Digital	we	HRD	Choose option	12/4/2025	2011-2477	
Assistant HR Manager's PC	Drive E	Local Disk C/ Asst. HR Manager/documents/HR Forms	Digital	e	HRD	Choose option	12/31/2025	2011-2477	

Showing 1 to 10 of 686 entries

Previous 1 2 3 4 5 ... 69 Next

Data Privacy

SECURITY

GENERAL

Home

Process Request

Data Sharing

Incident

COMPLIANCE REQUIREMENTS

Data Registry

5S Checklist

Data Inventory

DATA PRESENTATION

Compliance Check

Data Inventory

Physical & Digital Inventory

Storage *

Actual Location *

File Name/Description

Category Choose option

Security Status Choose option

Types Of Data Choose option

Retention Date dd/mm/yyyy

Backup Process

Submit

How Compliant are we?

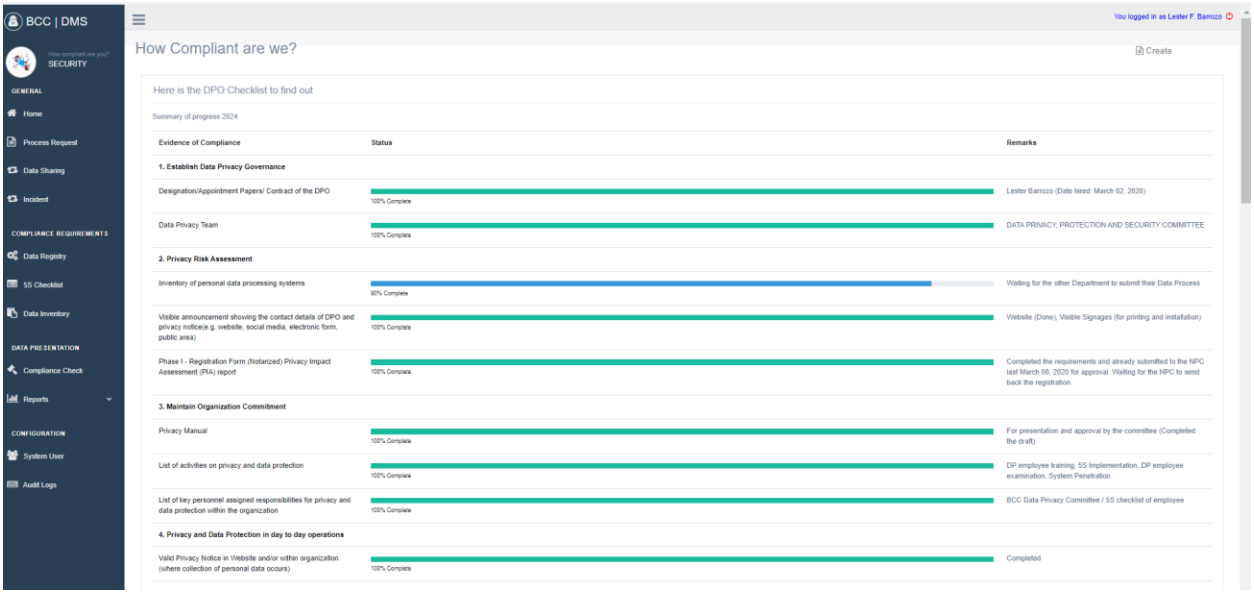
Create

Here is the DPO Checklist to find out

Summary of progress 2024

Evidence of Compliance
1. Establish Data Privacy Governance
Designation/Appointment Papers/ Contract of the DPO
Data Privacy Team
2. Privacy Risk Assessment
Inventory of personal data processing systems
Visible announcement showing the contact details of DPO and privacy notice(e.g. website, social media, electro form, public area)
Phase I - Registration Form (Notarized) Privacy Impact Assessment (PIA) report
3. Maintain Organization Commitment
Privacy Manual
List of activities on privacy and data protection
List of key personnel assigned responsibilities for privacy and data protection within the organization
4. Privacy and Data Protection in day to day operations
Valid Privacy Notice in Website and/or within organization (where collection of personal data occurs)
Consent forms for collection and use of personal data
List of Policies and Procedures in place that relate to privacy and data protection (may be in privacy manual)
Policies and Procedure in dealing with requests for information from parties other than the data subjects (media, enforcement, representatives)
Data subjects informed of rights through privacy notices, and other means
Form or platform for data subjects to request copy of their personal information and request correction
Procedure for addressing complaints of data subjects Certificate of registration and notification
5. Manage Security Risks
Data Center and Storage area with limited physical access
Report on technical security measures and information security tools in place
Firewalls used
Encryption used for transmission Encryption used for storage
Access Policy for onsite, remote and online access Audit logs

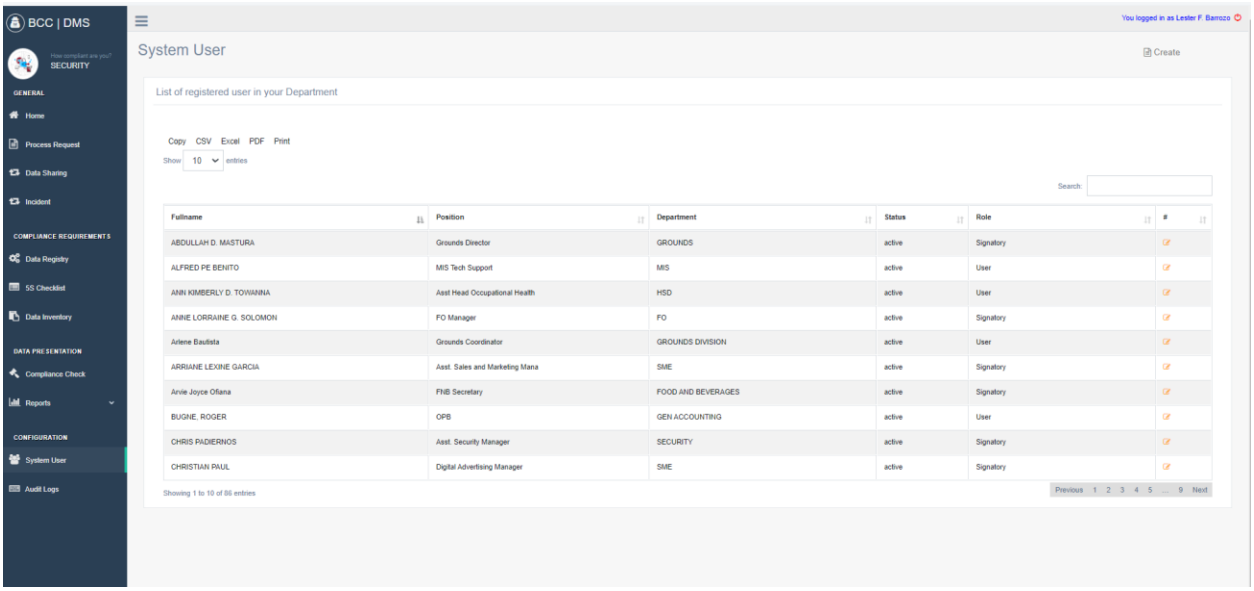
Evidence of Compliance
Back-up solutions
Report of Internal Security Audit or other internal assessments Certifications or accreditations maintained
Vulnerability Assessment
Penetration Testing for applications and network Other means to demonstrate compliance
6. Data Breach Management
Schedule of breach drills
Number of Trainings conducted for internal personnel on breach management
Personnel Order constituting the Data Breach Response Team Incident Response Policy and Procedure (may be Privacy Manual)
Record of Security incidents and personal data breaches, including notification for personal data breaches
7. Manage Third Party Risks
Data Sharing Agreements
List of recipients of personal data (PIPs, other PICs, service providers, government agencies)
Review of Contracts with PIPs
Review of Contracts for cross-border transfers Other means to demonstrate compliance
8. Human Resources Management
No. of employees who attended trainings on privacy and data protection
Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be pa employee files
Certificate of Training of DPO Certifications of DPOs
NDAs or confidentiality agreements Security Clearance Policy
9. Continuing Assessment and Development
Policy for Conduct of PIA (may be in manual)
Policy on conduct of Internal Assessments and Security Audits Privacy Manual contains policy for regular revie
List of activities to evaluate Privacy Management program (survey of customer, personnel assessment)
10. Manage Privacy Ecosystem
No. of trainings and conferences attended on privacy and data protection
Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards
No. of management meetings which included privacy and data protection in the agenda

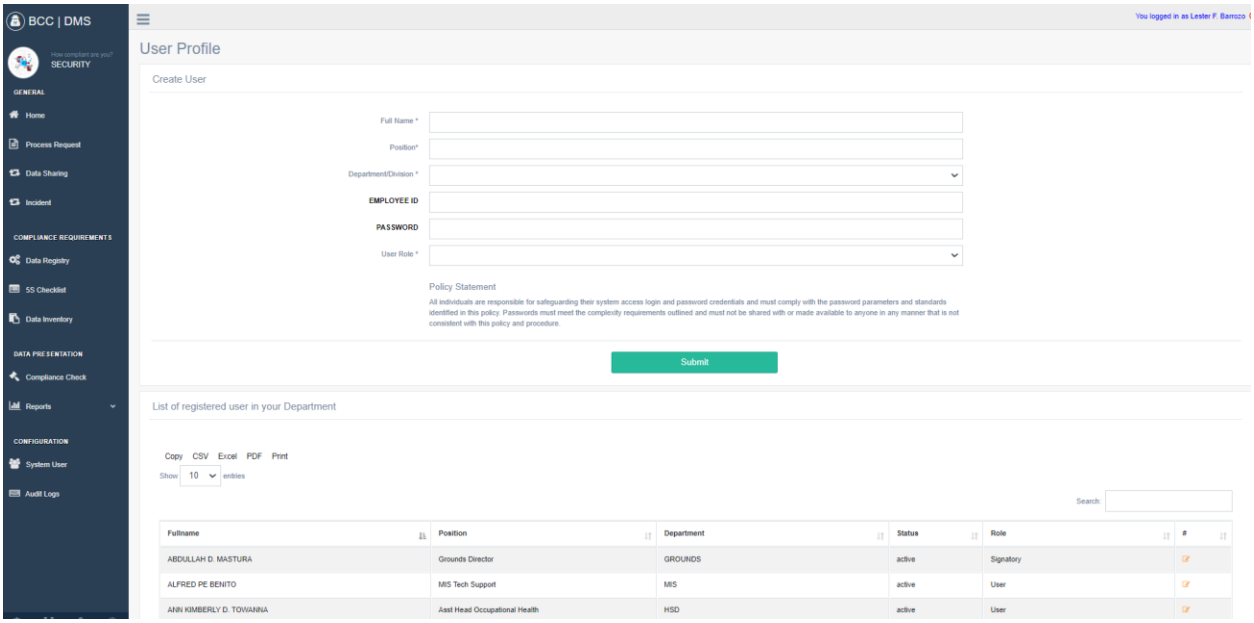


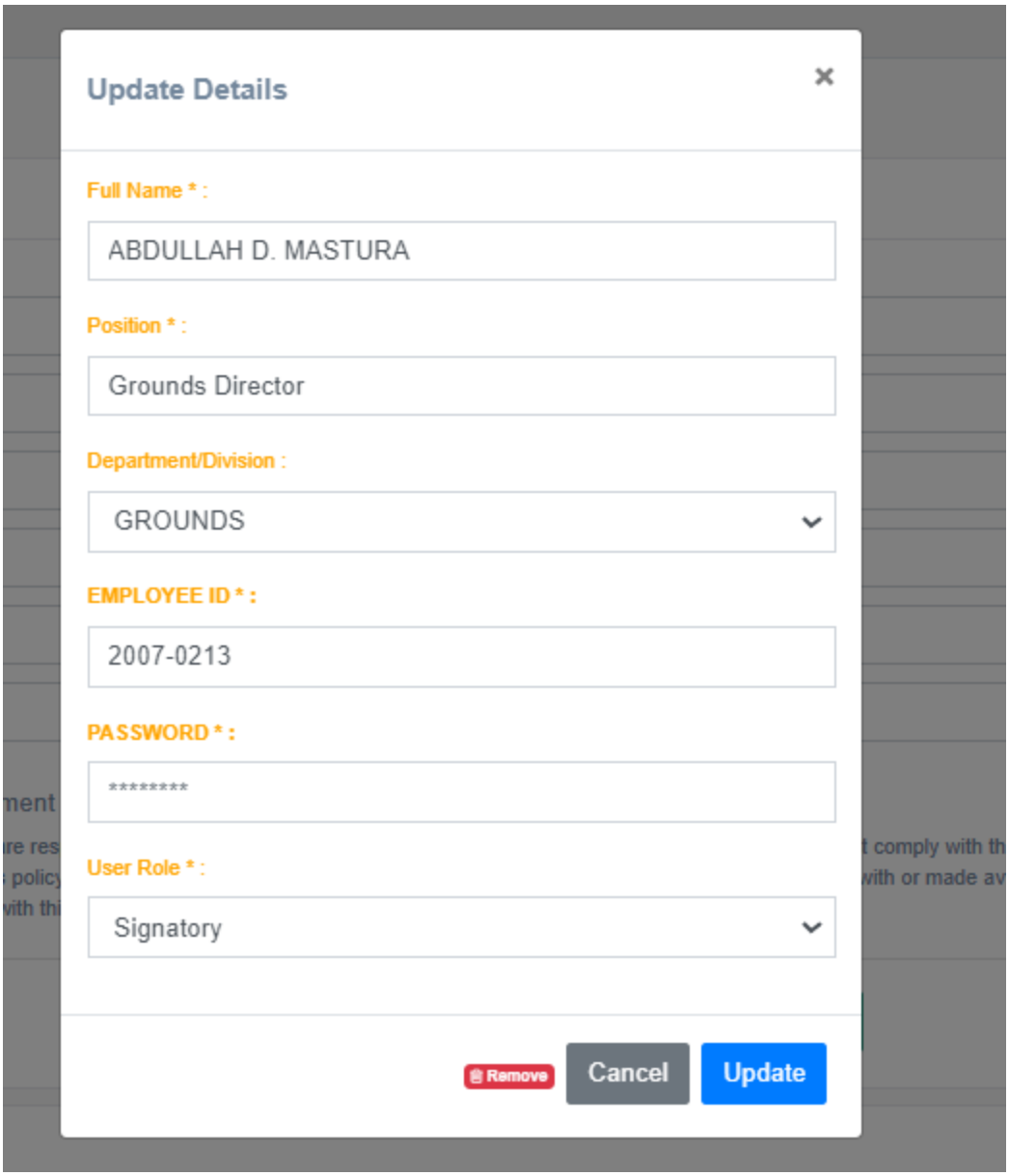
List of key personnel assigned responsibilities for privacy and data protection within the organization	100% Complete	BCC Data Privacy Committee / 5S checklist of employee
4. Privacy and Data Protection in day to day operations		
Valid Privacy Notice in Website and/or within organization (where collection of personal data occurs)	100% Complete	Completed
Consent forms for collection and use of personal data	100% Complete	Completed (Concern Department: HSD, HR, FNB, FO, Security)
List of Policies and Procedures in place that relate to privacy and data protection (may be in privacy manual)	100% Complete	Completed with memo
Policies and Procedure in dealing with requests for information from parties other than the data subjects (media, law enforcement, representatives)	100% Complete	Thru Data sharing agreement policy
Data subjects informed of rights through privacy notices, and other means	100% Complete	Thru electronic forms, verbal conversation.Orrientation of employees about this policy has been completed.
Form or platform for data subjects to request copy of their personal information and request correction	100% Complete	Data Privacy form is now available
Procedure for addressing complaints of data subjects Certificate of registration and notification	100% Complete	Policy is ready
5. Manage Security Risks		
Data Center and Storage area with limited physical access	100% Complete	Electronic door lock and authorization request to access this offices (MIS Office, PABX, Security Dept, Exec office)
Report on technical security measures and information security tools in place	100% Complete	Working with MIS
Firewalls used	100% Complete	BCC is using the MIKROTIK technology for securing the network.
Encryption used for transmission Encryption used for storage	90% Complete	Implementation is ongoing to every department (storage, email attachment)
Access Policy for onsite, remote and online access Audit logs	100% Complete	Policy for IFCA User, VPN for offsite, User access to devices, microsites
Back-up solutions	100% Complete	MIS backup policy for IFCA, email backup, (File drive backup server is on going)
Report of Internal Security Audit or other internal assessments Certifications or accreditations maintained	100% Complete	DPO template Report is available for (monthly and yearly)
Vulnerability Assessment	100% Complete	Completed the lists of the Clubs vulnerability with recommendation

Vulnerability Assessment	100% Complete	Completed the lists of the Clubs vulnerability with recommendation
Penetration Testing for applications and network Other means to demonstrate compliance	100% Complete	Working with MIS
6. Data Breach Management		
Schedule of breach drills	100% Complete	Working with HR / plan to start this activity on the first week of Feb 2021
Number of Trainings conducted for internal personnel on breach management	95% Complete	Working with HR / Not all employees attended the training
Personnel Order constituting the Data Breach Response Team Incident Response Policy and Procedure (may be in Privacy Manual)	100% Complete	Included in the DPO Manual / DATA PRIVACY, PROTECTION AND SECURITY COMMITTEE
Record of Security incidents and personal data breaches, including notification for personal data breaches	100% Complete	Report is ready (Monthly)
7. Manage Third Party Risks		
Data Sharing Agreements	100% Complete	Included in the DPO Manual, Data sharing template is available, Working with AKO System
List of recipients of personal data (PIPs, other PICs, service providers, government agencies)	100% Complete	Included in the DPO Manual (Data sharing template is available)
Review of Contracts with PIPs	100% Complete	To follow
Review of Contracts for cross-border transfers Other means to demonstrate compliance		To follow
8. Human Resources Management		
No. of employees who attended trainings on privacy and data protection	100% Complete	Working with HR
Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files	100% Complete	Included in the HR requirements
Certificate of Training of DPO Certifications of DPOs	100% Complete	Completed with certificate last August
NDAs or confidentiality agreements Security Clearance Policy	100% Complete	Need to double check with the management

8. Human Resources Management		
No. of employees who attended trainings on privacy and data protection	100% Complete	Working with HR
Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files	100% Complete	Included in the HR requirements
Certificate of Training of DPO Certifications of DPOs	100% Complete	Completed with certificate last August
NDAs or confidentiality agreements Security Clearance Policy	100% Complete	Need to double check with the management
9. Continuing Assessment and Development		
Policy for Conduct of PIA (may be in manual)	100% Complete	Using Electronic data management system
Policy on conduct of Internal Assessments and Security Audits Privacy Manual contains policy for regular review	100% Complete	Using Electronic data management system
List of activities to evaluate Privacy Management program (survey of customer, personnel assessment)	100% Complete	5S activity, Data Privacy training for new employee
10. Manage Privacy Ecosystem		
No. of trainings and conferences attended on privacy and data protection	100% Complete	1st batch has been completed last July 2020 / DPO attended 2 trainings online
Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards	100% Complete	Doing an online research and present recommendation to the management
No. of management meetings which included privacy and data protection in the agenda	100% Complete	DATA PRIVACY, PROTECTION AND SECURITY COMMITTEE meeting


BCC | DMS
How compliant are you?
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
You logged in as Lester F. Barroza
System User
Create
List of registered user in your Department
Copy CSV Excel PDF Print
Show 10 entries
Search:
Fullname
Position
Department
Status
Role
#
ABDULLAH D. MASTURA
Grounds Director
GROUNDS
active
Signatory
ALFRED PE BENITO
MIS Tech Support
MIS
active
User
ANN KIMBERLY D. TOWANNA
Asst Head Occupational Health
HSD
active
User
ANNE LORRAINE G. SOLOMON
FO Manager
FO
active
Signatory
Arlene Bautista
Grounds Coordinator
GROUNDS DIVISION
active
User
ARRIANE LEXINE GARCIA
Asst. Sales and Marketing Mana
SME
active
Signatory
Arvie Joyce Ofiana
FNB Secretary
FOOD AND BEVERAGES
active
Signatory
BUGNE, ROGER
OPB
GEN ACCOUNTING
active
User
CHRIS PADIERNOS
Asst. Security Manager
SECURITY
active
Signatory
CHRISTIAN PAUL
Digital Advertising Manager
SME
active
Signatory
Showing 1 to 10 of 86 entries
Previous 1 2 3 4 5 ... 9 Next


BCC | DMS
How compliant are you?
SECURITY
GENERAL
Home
Process Request
Data Sharing
Incident
COMPLIANCE REQUIREMENTS
Data Registry
5S Checklist
Data Inventory
DATA PRESENTATION
Compliance Check
Reports
CONFIGURATION
System User
Audit Logs
You logged in as Lester F. Barroza
User Profile
Create User
Full Name *
Position*
Department/Division *
EMPLOYEE ID
PASSWORD
User Role *
Policy Statement
All individuals are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.
Submit
List of registered user in your Department
Copy CSV Excel PDF Print
Show 10 entries
Search:
Fullname
Position
Department
Status
Role
#
ABDULLAH D. MASTURA
Grounds Director
GROUNDS
active
Signatory
ALFRED PE BENITO
MIS Tech Support
MIS
active
User
ANN KIMBERLY D. TOWANNA
Asst Head Occupational Health
HSD
active
User


Update Details
Full Name * :
ABDULLAH D. MASTURA
Position * :
Grounds Director
Department/Division :
GROUNDS
EMPLOYEE ID * :
2007-0213
PASSWORD * :
****
User Role * :
Signatory
Remove
Cancel
Update