

Compliance Audit Form

Organization Name: CyberNations// Protexxa

Audit Date: [23/04/2025]

Auditor Name: _____

Department/Unit Audited: Data Collection

Contact Person & Details: _____

Purpose of Audit: _____

Regulatory Frameworks Applicable (Check all that apply):

☐ Barbados Data Protection Act (BDPA)

☐ PIPEDA

☐ AIDA

☐ GDPR

☐ Other: _____

Section 1: Data Collection & Web Scraping (To be answered by Data Collection ONLY)

Data Sources & Collection Practices

Comments

1. List all primary data sources for cybersecurity job scrapes and data leaks.

2. Are there written guidelines your team follows to ensure data collection is legal and ethical? If not, are there plans to create such documentation?

☐ Yes/☐ No

3. Are TOS and robots.txt files checked and respected before attempting to collect data?

☐ Yes/☐ No

4. Are measures in place to minimize data collection to only what is necessary for your objectives?

☐ Yes/☐ No

5. How often are scripts reviewed or updated? Do you track issues so they can be used to improve processes?

6. Who is responsible for managing the API key used in data collection?

7. Are logs maintained for scraping activities (e.g., timestamps of scraping, data volume, source URL)? If yes, where are these logs stored?

☐ Yes/☐ No

8. Are there provisions for potential cease-and-desist requests to be documented and adhered to?

☐ Yes/☐ No

Total Score for Section 1: [/40]

Each 'Yes' = 5 pts, 'Partial/In Progress' = 3 pts, 'No' = 0 pts; N/A = not included in score.

Section 1 (PART 2): Data Cleaning & Processing (To be answered by Data Cleaning ONLY)

Data Integrity & Quality Control

Comments

1. Is there a structured data cleaning process that is version controlled or documented for reproducibility?

☐ Yes/☐ No

2. Are scripts or automated tools used to check data quality (e.g., duplicates, missing values, or formatting issues)?

☐ Yes/☐ No

3. How is missing data handled? Are nulls, blanks, and duplicates properly identified and managed?

4. After data cleaning, is the output reviewed manually or validated using tools to ensure accuracy before use?

☐ Yes/☐ No

5. How is potentially compromised or illegal data handled during cleaning (e.g., flagged, quarantined, discarded)?

6. Are cleaning rules reassessed regularly based on feedback, new patterns, or issues found?

☐ Yes/☐ No

7. Are there performance bottlenecks or known limitations in the current cleaning workflow?

☐ Yes/☐ No

Total Score for Section 1: [/40] **Add 5 to the final score**

Section 2: Data Storage, Security & Privacy

Security & Risk Awareness

Comments

1.If your team handles compromised or leaked data, how is risk managed during acquisition and storage. (3 pts max)

2. Are regular vulnerability assessments conducted? (3pts max)

☐ Yes/☐ No

3.Is there a centralized repository for finalized scripts and collected information or datasets? How is version control managed? (3 pts max)

☐ Yes/☐ No

4. Are backup systems in place for scripts, scraped information or datasets? Are they encrypted and stored offsite or in a secure cloud location? (4 pts max)

☐ Yes/☐ No

5.Is there a process for revoking access when a team member leaves or changes roles? (2 pts max)

☐ Yes/☐ No

6. Are there clear policies for retention and secure disposal? (3 pts max)

☐ Yes/☐ No

7.If datasets are stored across different platforms (e.g., Teams, GitHub, local machines), how is cross platform consistency ensured, so people are not working on outdated information? (3 pts max)

8. Are you aware of whether members have standard protections in place? Multi-Factor Authentication (MFA), etc.? (4 pts max)

☐ Yes/☐ No

Total Score for Section 2: [/25]

Section 3: Compliance & Accountability Measures

Breach & Incident Reporting

Comments

1.Are formal data breach reporting processes in place?

☐ Yes/☐ No

2.Any compliance violations or incidents before this audit?

☐ Yes/☐ No

3. Is there a documented incident response plan in case of a data breach or unauthorized access? If yes, who is responsible for executing it?

4.Has your team encountered any challenges in storing or organizing data securely (e.g., decentralized files, missing logs, lost local data)?

☐ Yes/☐ No

5.Is there a dedicated person responsible for ensuring your team remains up to date on compliance obligations?

☐ Yes/☐ No

Total Score for Section 3: [/25]

Section 4: Continuous Improvement & Compliance Culture

Transparency

1.Has your team finalized a document outlining the roles and responsibilities of each subgroup or team member?

☐ Yes/
☐ No

Comments

2. What specific improvements (if any) has your team made in the past 3–6 months to strengthen data practices and compliance?

3.Do you conduct internal reviews or debriefs after completing major collection or cleaning cycles?

☐ Yes/
☐ No

4.When was the last time your team reviewed or discussed compliance expectations in a meeting or formal setting?

5.What tools or support do you feel would help your team become more compliant or secure?

Total Score for Section 4: [/10]

For Official Use Only:

Section 6: Continuous Improvement & Recommendations




Best Practices & Future Improvements

Feedback Area	Compliance Risk Level	Suggested Action	Responsible Party	Deadline	Status
What audit findings are being addressed?	High, medium, limited, low, minimal risk, etc.	What corrective action is proposed?	Who owns the action?	By when?	Open, Closed, In progress, etc.

Final Compliance Score Calculation

Each 'Yes' = 5 pts, 'Partial/In Progress' = 3 pts, 'No' = 0 pts; N/A = not included in score.

Section	Max Score	Score Achieved	Compliance Status
Data Collection	40	[]	[]
Data Cleaning & Processing	40	[]	[]
Data Storage, Security & Privacy	25	[]	[]
Compliance & Accountability Measures	25	[]	[]
Continuous Improvement & Compliance Culture	10	[]	[]
Total	100	[]	[]

Compliance Score (%)	Final Rating
90 - 100%	 Compliant – No major risks, minor improvements suggested.
70 - 89%	 Partially Compliant – Some risks identified; action needed.
Below 70%	 Non-Compliant – Does not meet requirements; immediate action is required.

Final Rating: []

Auditor's Signature:

Witness Signature:

Team Lead's Signature:

Date: