DATAPHORIA

Questions to Ask When Building Your IT Security Policy

FIA ORGANISATIONAL MEMBER

1300 537 787
info@dataphoria.com.au

DATAPHORIA

Contents

DISCLAIMER

While Dataphoria are not cybersecurity experts or lawyers, data security is at the heart of everything we do. This guide is designed to assist you in asking smart questions when building your internal Security Policy - this is not legal advice!

Spot the Difference: Policy Essentials

PRIVACY POLICY

Your Privacy Policy is your outward facing policy, which should show the public how you meet your obligations under the Privacy Act. Additionally, if you are an APP entity, you are bound by the Australian Privacy Principles to have a valid privacy policy, answering a range of key questions.

SECURITY POLICY

Your IT Security Policy should be an internal document, showing how you will manage your systems and processes in such a way as to meet the obligations of your Privacy Policy. For example, if your Privacy Policy states data will not be transferred overseas, your IT Security Policy should note where you are happy to hold data, noting that some cloud service providers do not offer the options to host in Australia.

EMPLOYEE IT POLICY

Your Employee IT policy should note employee obligations and consequences for misuse. It should include sections for all areas of duty of care, according to related laws governing the use of devices and related data. Know that your team and their devices are your weakest links. Organisations with great cybersecurity and IT policies can still get hacked due to human error.

Policy should be the blueprint when designing a system to protect one of your most valuable assets: **your data**.

There are some great policy templates online that can act as a starting point for the type of fundraising organsation you are.

1300 537 787
info@dataphoria.com.au

IT SECURITY CHECKLIST

DATAPHORIA

ACCESS AND STORAGE	
Questions to Ask	**Response**
Where will your confidential and/or personally identifiable information (PII) be held?	
Which devices will have access to PII?	
Do you have an up-to-date inventory of devices with access to PII?	
Are there different rules for personally owned (BYO) devices and devices owned by your organisation?	
Can you ensure that PII cannot be not stored on personal devices, as this would make it harder to track and delete (if required)?	

ENCRYPTION

Ideally, software and hardware encryption should be used across all devices and files. Laptops can be encrypted with hard drive encryption solutions like Bitlocker, and files can be password protected (especially in transit).

THEFT RISK	
Questions to Ask	**Response**
What security measures will you take to avoid risk from theft?	
How will the data be encrypted at rest?	
Will data be secured under lock and key, with access controls provided and logged on a need-to-access basis?	
Can this be executed for employees working from home/remotely?	
Will data be centrally held on premises or in a cloud?	
Where risks are higher, how can access points be limited? *For example: If working with an overseas call centre, you could consider organising a dialler that enables users to view/access only one record at a time, with screenshots/screensharing disabled. This effectively enables data to be shared without being held.*	

ON PREMISES VS THE CLOUD

We would recommend to thoroughly research your options before working with any 3rd party, but a secure cloud service provider with professional access controls is ideal (eg. AWS or Microsoft Azure).

IT SECURITY CHECKLIST

DATAPHORIA

SENSITIVE DATA	
Questions to Ask	**Response**
Will the policy have differing rules for Sensitive data?	
What additional security policies will you have in place to address Sensitive data?	

'Sensitive data' is subject to a higher level of privacy protection. For your Privacy Policy, you may wish to consider addressing the collection and usage of Sensitive Data separately to data that is collected for the purpose of fundraising.

DATA IN TRANSIT	
Questions to Ask	**Response**
How will data be protected in transit?	
What types of encryption and software delivery solutions will be employed?	

DATA RETENTION AND DELETION PROCESS	
Questions to Ask	**Response**
Is there a process designed to permanently delete the PII of an individual, when requested?	
How will this be managed across all data systems? (e.g. email service provider, CRM, finance package, backups, 3rd party providers).	
How long should each type of data be retained?	
Should data be de-identified after a set period of time?	
Can Sensitive Data be deleted after a set period of time?	
Can you ensure that data is deleted permanently?	
How will "deleted" be defined?	
Where there is risk that deleted data can be recovered, is there an option to overwrite data/destroy the related hardware and remove data from all related backups?	

IT SECURITY CHECKLIST

DATAPHORIA

EMPLOYEE IT POLICY	
Questions to Ask	**Response**
What software can and can't be downloaded onto devices owned by the organisation? eg. *Spotify may be OK, whereas you may need to restrict any software allowing remote access by third parties -for example, online proctoring software for digital exams.*	
Who can use devices owned by the organisation?	
Can employees access data using personal devices? *Consider risks around family members and friends sharing a personal device.*	
Do passwords for all user accounts meet minimum requirements (15 characters or more, using letters, numbers and symbols), with multi-factor-authentication enabled?	
What are the acceptable personal uses of a device owned by the organisation? What types of websites can and can't be browsed?	
Does business software need to be installed on a personal device for IT security (eg Microsoft Authenticator or Company Portal)?	
What actions are prohibited?	
What types of surveillance is required? *eg Technical surveillance of email, user logs* *Physical surveillance (security cameras, biometric security)*	
In the case of a suspected breach or on departure from a business, will personal devices require access by the organisation?	
In the case of a suspected breach, does the organisation have the ability to erase data on a personal device?	

IT SECURITY CHECKLIST

DATAPHORIA

ACCESS POLICIES - INTERNAL	
Questions to Ask	**Response**
Have all employees signed off on the Employee IT Policy before gaining access to IT infrastructure?	
Does the business have the ability to remote delete data held on a business / personal device?	
Will PII / confidential / sensitive information be accessible from personal devices? What steps will be taken to protect data in these circumstances?	
Will all access be logged?	
What password policies and multi-factor authentication policies will be in place?	
Will users need to regularly change passwords? *Note: Microsoft now advises against changing passwords regularly as it encourages use of weak, memorable passwords.*	
What types / makes of device will be acceptable?	
Will devices need anti-virus software installed?	
Will emails be scanned by software for phishing and virus risk?	
Will devices need to be hardware encrypted?	
Will software updates and patches be remotely installed by the business or will the user be responsible for installing updates? If the user is responsible, how will this be monitored?	
Will centralised IT management solutions be employed? For example, Intune can remote deploy IT policies and remote delete business data stored on all related devices.	
Which team members should have access to which types of data? What training should be provided accordingly?	

IT SECURITY CHECKLIST

DATAPHORIA

ACCESS POLICIES – EXTERNAL	
Questions to Ask	**Response**
How will data be protected when held by 3rd parties, or if remote access is used?	
Who will audit the IT security policies of the related 3rd parties?	
What references can be requested to ensure good business practices?	
What legal documentation should be in place before any data is shared with the 3rd party?	

Before sharing data with another party, a standard Mutual Confidentiality deed or Provision of Services Agreement should be organised and agreed.

MICROSOFT 365	
Questions to Ask	**Response**
Is multi-factor authentication enabled for all accounts?	
Are Conditional Access policies in place so only managed devices can connect to your tenant?	
Can non-managed devices access your accounts and data?	

Conditional Access policies allow you to only enable managed devices (with Azure AD joined and Intune enrolled) to connect to your Microsoft 365 tenant. Even if a users' credentials are compromised, an attacker won't be able to access your account because their device isn't Trusted.

IT SECURITY CHECKLIST

DATAPHORIA

INCIDENT PLAN	
Questions to Ask	**Response**
In the event of a hack, physical disaster or any other type of data loss, how will business continuity be managed?	
How will be data be backed up and recovery tested, prior to any real threat?	
In the event of a disaster, what process will be undertaken to notify 3rd parties, donors and customers?	
How will the related data be stored to enable this process?	
How will the business respond to a ransomware threat?	

Beyond the Checklist

MFA ALONE IS NOT ENOUGH

It's important, to note that MFA alone is no longer enough. Attackers have developed bypass techniques to gain access to your account and data, so we need to take additional precautions.

Here's a little advice from Chuong Mai Viet, the Managing Director at Fuse Technology, a trusted IT solutions provider we have used for systems hardening projects:

- If you haven't already enabled multi factor authentication for all accounts in your Microsoft 365 tenant – do it **RIGHT NOW**!
- Set up Conditional Access policies to only enable Trusted Devices (with Azure AD joined and Intune enrolled) to connect to your Microsoft 365 tenant.
- Even if a users' credentials are compromised, an attacker won't be able to access your account because their device isn't trusted.
- Using Trusted Devices with a secure user account (with a strong password and MFA enabled) significantly reduces the likelihood of account compromise and improves data loss prevention capacities.

BUILDING A SECURITY-SMART CULTURE

A secure business starts with a risk-aware team, and cyber security is a team sport. Build a security focused culture by simulating regular phishing attacks and rewarding your team for reporting. Your team will be more likely to question what to open and where an email originates from.

Beyond the Checklist

CONSIDER CYBER-INSURANCE

Cyber-insurance is increasingly expensive, in line with ever increasing risks from sophisticated scammers, but it can be a solid investment.

The additional benefit will be in the form of the IT auditing performed by your underwriter. This will often highlight key areas of risk that you should mitigate.

TEST, TEST, TEST

Hiring a reputable 3rd party to run an audit on your IT infrastructure and perform a penetration test will help you see where to focus your attention. Make sure you have a confidentiality agreement in place with any provider prior to allowing any access to your systems.

If you do undertake IT hardening projects, try to "break them" once they are deployed. Setting up security measures is not an easy task, so it pays to test them yourselves

Questions about Privacy?

Download your free fundraising privacy toolkit here, built in association with FIA and PFRA: https://www.dataphoria.com.au/privacy_toolkit/

MEET ALEX HARDING.

Alex founded Dataphoria in 2009, to provide clients with better leads for better results.

His passion is in leveraging disparate data points to build responsive data sets, when solving marketing challenges.

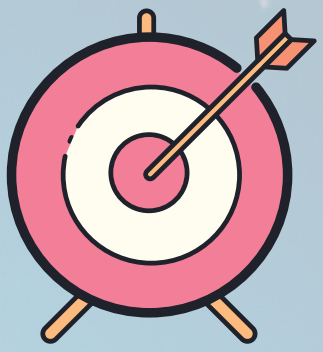
Demonstrating his nerdiness, you actually need to pass a maths test to become an employee of his business.

FIA ORGANISATIONAL MEMBER

1300 537 787
info@dataphoria.com.au

Solutions for Charities

DATAPHORIA



TARGETED MARKETING LISTS

Identify and target individuals most likely to respond to your cause, based on demographics, psychographics and behavioural data or donor lookalikes.

- Costs no more than RRP
- Trusted by many of Australia's top fundraising call centres and charities
- Strategy, de-duplication and optimization
- Full data bureau services available

LEAD GENERATION

Your calling campaign can be designed to target engaged consumers, ready for direct regular giving conversion.

Dataphoria have generated **hundreds of thousands** of opt-in leads for charities for over ten years.

- No management fees or long term contracts - pay per lead
- Bespoke multichannel campaigns
- Real time data processing
- Continuous optimisation

ANALYTICS & DATA STRATEGY

Our focus is on building solid data strategy around the goals of our clients.

- Understand your donors and predict future behaviour
- Predictive modelling to identify upsell and cross-sell opportunities
- Establish risk of churn
- Reactivation segmentation

PRIVACY

Dataphoria are a trusted partner of the FIA and PFRA on Privacy guidance and training.

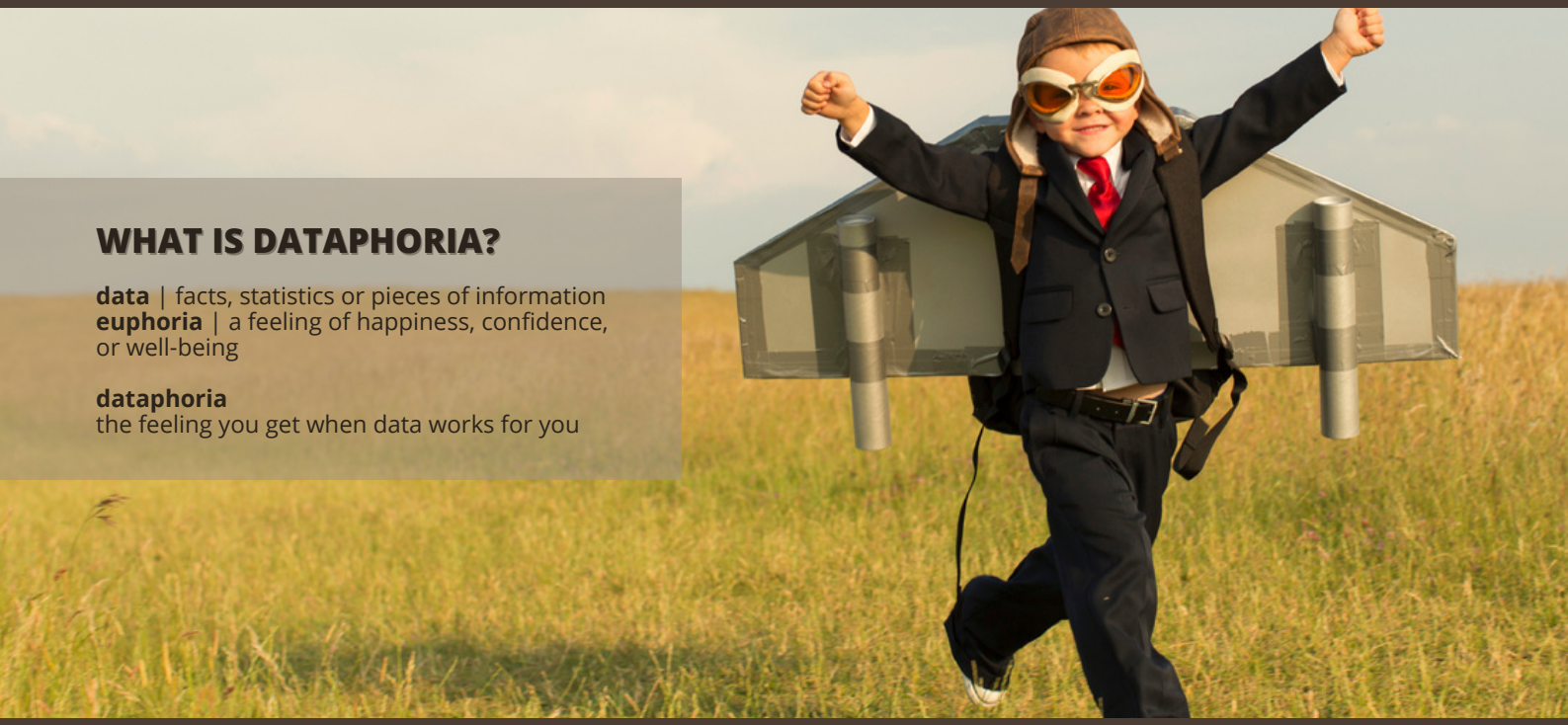
- Full auditing and accreditation process for all suppliers
- Consumer care line
- Online opt-out facility
- Personal data legislation warranties provided

CONTACT US TODAY

1300 537 787
info@dataphoria.com.au

DATAPHORIA

NOT-FOR-PROFIT DATA-DRIVEN MARKETING



WHAT IS DATAPHORIA?

data | facts, statistics or pieces of information
euphoria | a feeling of happiness, confidence, or well-being

dataphoria
the feeling you get when data works for you

WHAT PEOPLE SAY

"It is refreshing to work with a professional organisation that demonstrates equal passion and commitment to helping solve your business challenges.

Working with Dataphoria reduces my risk as I know that the solutions and data provided are of high integrity. I work with them not only for supply of external lists but also to consult on the most effective means of reaching our sophisticated and diverse audience."

Kylie Allison
Acquisition Marketing Specialist
Australian Institute of Company Directors

"Dataphoria were very proactive in suggesting enhancements to our offering, along with new opportunities and ideas. They were really conscious of delivering value and ROI, taking learnings from the commercial world and testing in the NFP sector with reduced risk. They really live up to their name, with a strong focus on analytics and data-driven insights, and they approached our relationship as a partnership.

I would highly recommend Dataphoria, and hope to work with them again in my future roles and organisations."

Rachael Lance
National Manager of Individual Giving
Make-A-Wish Australia

"Dataphoria add real value with strategies around data discovery that only come from deep experience across thousands of unique client briefs. I'm delighted to recommend Dataphoria to my clients, because they have access to the deepest and broadest data sources available in the Australian market and beyond.

I get an independent view of the data landscape rather than using a provider directly that pushes their own and often limited view of the market place."

David Barlow
Regional Sales Director
Flat Planet

FIND OUT HOW WE CAN ASSIST

1300 537 787
info@dataphoria.com.au