Painted Dog Research

Data Security Policy

03 September 2019

A bit about the market research industry and us

Painted Dog Research (PDR) is a small marketing research consultancy that conducts surveys and group discussions on behalf of client organisations (The Client).

The research we conduct rarely requires us to use client customer data. Most of the research that we conduct utilises primary data – that is, deidentified data collected directly from the public (via telephone, online or face to face) under the guarantee of privacy and confidentiality.

Contents

Certifications, Assessments and Audits

Certifications, Assessments and Audits

1. Is the provider currently compliant with ISO 27001/2?

Although Painted Dog Research does not hold ISO 27001 accreditation, it is compliant with most of the ISO 27001 accreditation requirements.

In instances where we do not comply, we do not deem it to be strictly necessary in our line of business.

We wish to point out that should The Client deem it necessary for Painted Dog to comply in ANY areas, that Painted Dog would be willing to invest the required time and money to comply in order to continue to do business with The Client.

2. If currently not compliant, does the provider have plans to become compliant with ISO 27001/2?

Painted Dog Research will only seek ISO 27001 accreditation if The Client deems it is necessary as part of doing business with us.

If not mandatory, Painted Dog will remain compliant with the ISO standards, but is unlikely to undertake the investment required to achieve formal accreditation.

3. Does your organisation hold any other relevant certifications?

Painted Dog currently holds ISO 20252 accreditation. This accreditation is directly relevant to Market, Opinion and Social Research. It covers many aspects of market research including most of the same standards relating to the handling of data as requested by The Client.

4. Do you perform regular vulnerability assessments of your service? Do you share the results?

Painted Dog performs monthly network and system penetration tests for vulnerability. The results of these tests are not shared publicly, however due to the amendment to the Privacy Act legislation, from 22 February 2018, PDR will comply with the amendments, and any data breaches will be shared publicly. All tests are conducted by independent IT firm, CBM Corporate.

5. Do you allow The Client to perform independent vulnerability assessments?

Painted Dog does not currently allow The Client to perform independent tests, however we would be open to discussing this should The Client wish to do so.

6. Do you conduct regular ISO audits?

Painted Dog is annually audited as part of its ISO 20252 accreditation by an independent auditor (BSI International). Quarterly self audits are also conducted by Painted Dog as part of this ISO accreditation process.

Privacy and Confidentiality

Privacy and Confidentiality

1. Do you have a published privacy policy? Please include location.

Yes, Painted Dog has a published privacy policy. This is available at: https://painteddogresearch.com/privacy-security

2. Are there any laws in the country where the data is stored that may affect the privacy and/or confidentiality of that data?

All client data is currently stored in Australia. Although Painted Dog has an office in Bristol, England, no data is stored on premise. It is accessed by secure VPN.

Data Security

Data Security

1. Are customers logically or physically separated from each other? What controls are in place to prevent accidental access to data?

Painted Dog's clients are not provisioned to access any data or information stored within our IT infrastructure. Therefore there is no chance of any client getting access to another clients' data.

2. Who owns the data contained within the hosted environment for each customer?

Painted Dog has responsibility for the data that is stored within its hosted environment. If a client asks Painted Dog to destroy or return its data, we will comply immediately.

3. Is data encrypted at rest?

Data stored locally within our IT infrastructure is not encrypted at rest. Access to this data however is protected through multifactor authentication systems, securely encapsulated by Secure Socket Layer (SSL) sessions.

4. Is data encrypted in transit?

Yes, data that is sent to our secure offsite facility is encrypted and encapsulated within a Secure Socket Layer (SSL) session.

5. Is the integrity of the data regularly tested?

Yes, Painted Dog conducts periodic data recovery and disaster recovery tests. File recovery is tested regularly, however disaster recovery is only conducted annually.

6. Describe the backup regime used, including any offsite backups

Continuous (3 hourly) delta incremental backups of all systems, information and data, replicated offsite through a Secure Socket Layer (SSL) session.

7. Are backups encrypted?

Yes, backups are encrypted and in addition there is NAS NTFS access restriction via a username and password.

8. Are there any additional costs associated with Data recovery or extraction of data?

Yes, Painted Dog incurs additional costs for data recovery and extraction of data, however these costs are entirely borne by Painted Dog and not passed onto The Client.

9. What is the average recovery time for data restoration?

For complete site loss, such as in the event of a fire, recovery could take 1-2 days depending on engineer availability. However, for server or file loss the recovery time is approximately 2 to 4 hours.

10. Is administrative access to data logged and audited?

Administrative access is logged and audited. Furthermore, administrative access is limited to all IT infrastructure and all IT systems. All secure access passwords are changed annually, and all access on site and remote is logged. Only two parties have access –CBM and Justin Scerri - an owner and founder of Painted Dog Research.

11. What security controls are in place for access to the data?

Access to data at Painted Dog requires multifactor authentication. Any network access also requires a username and password. Password policies also apply which require all users to change their password every 60 days meeting minimum security requirements such as alpha-numeric, including caps, and no repeatable passwords. Additionallly, Painted Dog employs 2 Factor Authentication for all Office 365 applications.

When staff of Painted Dog leave its employ, their network access is locked immediately.

12. What controls are in place to detect and respond to network based attacks (eg IPS, monitoring)

PDR has invested in a Layer 4 Next Generation Firewall. This appliance allows detection, remediation, alerting and reporting across most network and internet borne attacks.

Painted Dog also has modern Sophos Antivirus Software with virus definitions that are updated hourly.

Physical Access to the Data Centre

Physical Access

1. Describe the physical security employed at your Data Centres (eg Armed Guards, CCTV, Access controls etc)

Entry to the Painted Dog building is restricted to those with an electronic security FOB. This device gives access to the building and lift; however a physical key is also required to gain access to our office area. Logs are available for every individual who has used their security device to enter the building.

All data is stored in a locked and physically secure comms rack. Only three staff have access to the key for this rack.

Painted Dog also has CCTV security surveillance within its office space overlooking entry/exit, server access and key entry points throughout the building.

2. Describe the access controls at your Data Centres (eg biometric security)

During work hours nobody is granted access to the Painted Dog office without receiving signed security access from our reception team (security diary). Again, there is locked access to Painted Dog's building, office and comms racks.

3. Provide details on screening of administrative staff (eg integrity checks, police clearance etc)

When employing administrative staff they are typically given Police Checks, Working with Children checks, Employment Checks (past employers) and Character Referee Checks (via personal references).

All admin staff at Painted Dog have worked here for a minimum of 5 years.

Data Retention and Disposal

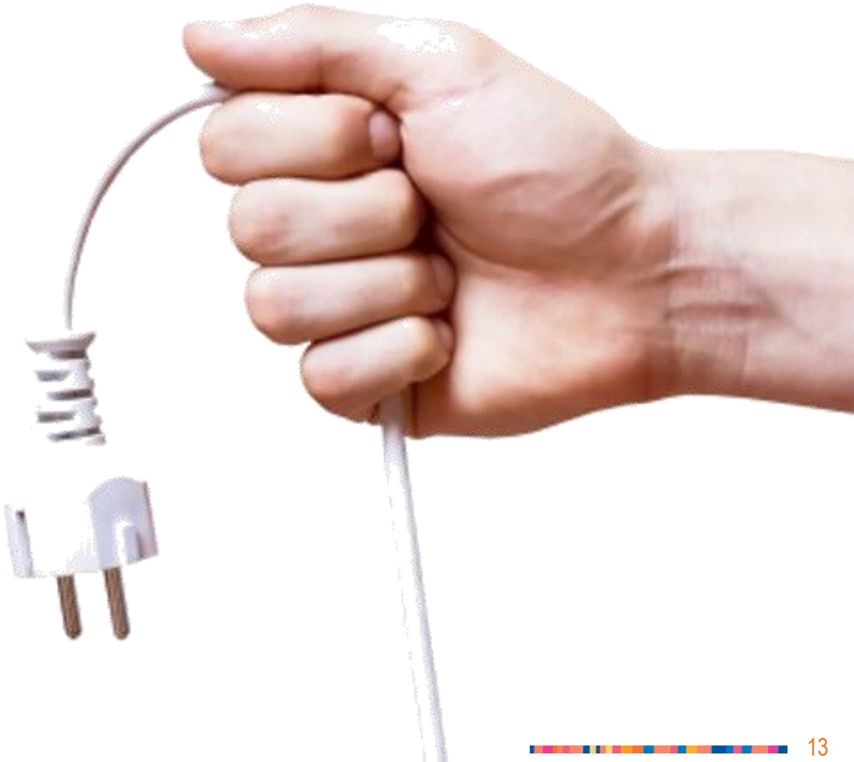
Data Retention and Disposal

1. Is data retained by the provider after the subscription is discontinued? If yes, how long?

Painted Dog disposes of all individually identifiable, personal data 12 months after it has been used.

2. Can you provide a certification to confirm that data was deleted after the subscription is discontinued?

We currently do not provide certification after data has been deleted, however, we would be willing to provide certification should it be required. Provision of a certificate may incur a fee that would be passed onto The Client.



Availability Service Levels

Uptime and Availability

1. Uptime Level

Painted Dog has 24 hour, 7 days per week uptime availability and has achieved this for 98% of the time over the past 10 years, excluding planned maintenance periods.

2. Recovery Time Objective

Recovery time varies depending on the type of disaster encountered. For complete site loss, such as in the event of a fire, recovery SLA is 1 to 2 days depending on replacement hardware availability. However, for server or file loss the recovery time is approximately 2 to 4 hours.

3. Recovery Point Objective

Painted Dog IT systems are backed up through the leveraging of best practice Disaster Recovery product suites, which enable for a multi generational recovery point objective. Painted Dog's systems backup processes encompass multiple daily data deduplication delta file backups, performed at the hardware layer of storage infrastructure.

Depending on the type of disaster, the recovery point will vary, and in case of total asset and site loss, the recovery point objective will be the previous business day delta backup from 6:00 pm. For file or sever loss, the recovery point will be within 3 hours of the loss.

4. Planned Maintenance

Painted Dog has implemented various levels of planned maintenance. It conducts server maintenance on a monthly basis, end user PC/notebook maintenance on a monthly basis, and also has in place a number of automated policies to implement critical/important updates automatically on every machine.

Other maintenance procedures such as updates of viral definitions occurs hourly every day.

Painted Dog Research has a Service Level Agreement with CBM Corporate to perform most of this maintenance work.

5. Are there any penalties to not meeting the above SLAs?

There are no penalties to Painted Dog for not meeting these Service Level Agreements because most of our service level requirements relate to the provision of research services and not IT services.

There are penalties and clauses in our contract with CBM Corporate should they fail to meet the SLAs that we have with them.

Notifications

Notifications

1. Do you notify customers of upcoming planned maintenance and upgrades?

Scheduled maintenance upgrades are controlled through a change management process, which require prior testing and approval from senior Painted Dog management. These activities are conducted outside of business hours and are planned to never directly impact our customers or their data. As part of the change management process, appropriate roll back strategies are employed to manage and mitigate change management risks.

2. Do you notify customers in the event of a security breach?

Painted Dog Research would notify its customers immediately if we experienced a security breach that resulted in private client information being illegally accessed. Mentioned previously, Painted Dog will also comply with amendments to the Privacy Act from 22 February 2018. We also have a separate Incident Response Plan.

Hunt Smarter.