DATA PROTECTION AND SECURITY POLICY
FOR
DIGIPIXEL

Version No.:	1.0
Date:	15/01/2024
Prepared By:	Mr. Dave Gurbani
Reviewed By:	Mr. Tan Yong Li
Approved By:	Mr. Tan Yong Li

Change History Log

S/N	Version	Release Date	Updated By	Summary of Changes	Reviewed By	Approved By
1	1.0	15/01/2024	Mr. Dave Gurbani	Initial release.	Mr. Dave Gurbani	Mr. Tan Yong Li

TABLE OF CONTENTS

1 OBJECTIVE

The objective of this Data Protection and Security Policy ("**policy**") is to serve as a basis and standing instructions upon which Digipixel ("**we**", "**us**", or "**our**") provides for baseline data protection and security controls in our company in accordance with the guidelines set out in the Personal Data Protection Act ("**PDPA**"). It sets out the basis upon which we may use, collect, disclose, or otherwise process personal data of employees, job applicants and customers in accordance with the PDPA. This Policy also applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose, or process personal data for our purposes.

2 SCOPE

The scope of this Policy to set clear guidelines and instructions governing both Data Protection and Data Security in our company over personal data of customers, employees, job applicants and our proprietary/critical business-related information.

This notice applies to all persons engaged in a contract of service with us (whether on a part-time, temporary or full-time basis) and interns and trainees working at or attached to us (collectively referred to as "**employees**"), and all references to "**employment**" shall apply equally to internships, traineeships (as may be applicable). It also applies to all persons who have applied for any such job positions with us ("**job applicants**"). Furthermore, this Policy shall also apply to individuals ("**customers**") who (a) has contacted us through any means to find out more about any goods and services we provide, or (b) may, or has, entered into a contract with us for the supply of any goods or services by us or our vendors.

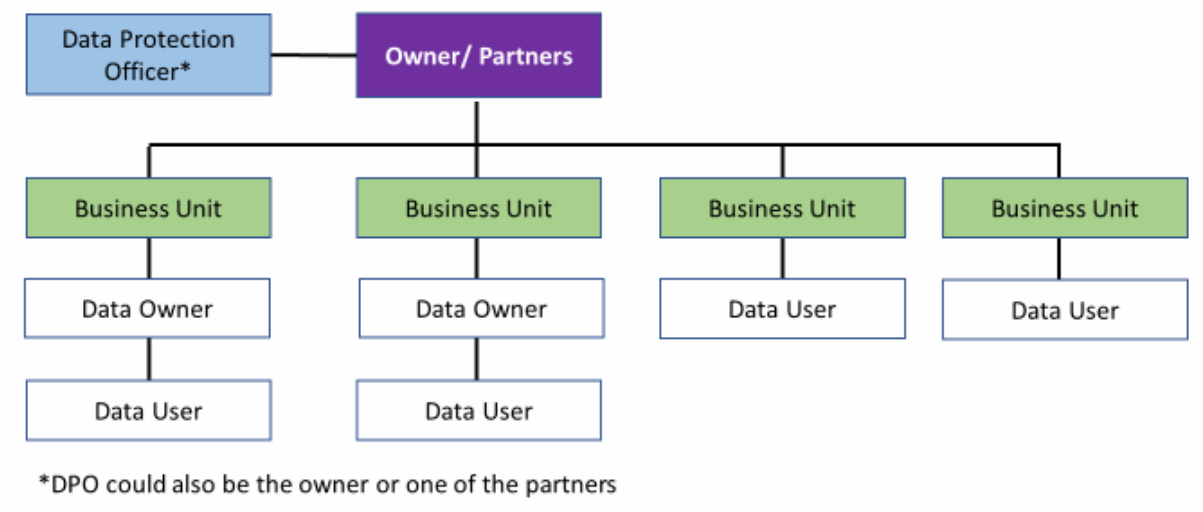
As used in this Policy, "personal data" means data, whether true or not, about an employee, job applicant or customer who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

3 GOVERNANCE STRUCTURE

○

3.1 Sole-Proprietor/Partnership Reporting Structure

The below diagram demonstrates a reporting structure for sole-proprietors or partnerships which incorporates data protection into its implementation.



Role	Responsibilities	Person-in-charge

Owner/Partners	• Embed data protection and security within the organisation's governance structure to set the direction, values and course of actions • Designate members who are responsible for implementing and managing data protection and cybersecurity programme and initiative • Approve and review organisation's governance framework and risk management structure • Appointing and empowering the DPO • Allocating resources (e.g. budget, manpower) to data protection and security • Update and review of organisation's governance performance and risk reporting • Provide strategic guidance on the implementation of data protection and security initiatives	TAN YONG LI
Data Protection Officer[1]	• Ensure compliance of PDPA when developing and implementing policies and processes for handling personal data • Promote importance of data protection and security practices and communicate personal data protection and security policies to all staff • Handle access and correction requests to personal data, and manage related queries and complaints • Alert owner/ partners to any risks that might arise with regard to personal data • Establish and review risk reporting structure and implement monitoring measures (e.g. internal audit) to evaluate effectiveness	DAVE GURBANI

Data Owner	• Compliance with the PDPA and DPP, for PD within their charge and possession • Seeking approval with their respective BU Heads regarding the requirements for the management of the PD • Updating the DIM when new categories of PD are collected, used or disclosed	BU Heads
Data User	• Compliance with the PDPA and DPP, for PD they have access to	TAN YONG LI

[1]Owner may also double-hat as Data Protection Officer.

4 POLICY

4.1 Data Protection

4.1.1 Employees

This Data Protection Notice ("**Notice**") sets out the basis upon which Digipixel ("**we**", "**us**", or "**our**") may collect, use, disclose or otherwise process personal data of employees in accordance with the Personal Data Protection Act ("**PDPA**"). This Policy applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.

APPLICATION OF THIS NOTICE

1. This Notice applies to all persons engaged in a contract of service with us (whether on a part-time, temporary or full-time basis) and interns and trainees working at or attached to us (collectively referred to as "**employees**"), and all references to "**employment**" shall apply equally to internships and traineeships (as may be applicable).

PERSONAL DATA

2. As used in this Notice, "**personal data**" means data, whether true or not, about an employee who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

3. Personal data which we may collect in the context of your employment with us includes, without limitation, your:

(a) Name or alias, gender, NRIC/FIN or passport number, date of Birth, nationality, and country and city of birth;
(b) Mailing address, telephone numbers, email address and other contact details;
(c) Employment and training history;
(d) Salary information and bank account details;
(e) Details of your next-of-kin, spouse and other family members;
(f) Work-related health issues and disabilities;
(g) Records on leave of absence from work;
(h) Photographs and other audio-visual information;
(i) Performance assessments and disciplinary records; and
(j) Any additional information provided to us by you as a job applicant (that is, prior to being engaged as an employee)

4. Other terms used in this Notice shall have the meanings given to them in the PDPA (where the context so permits).

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

5. We generally collect personal data that (a) you knowingly and voluntarily provide in the course of or in connection with your employment or job application with us, or via a third party who has been duly authorised by you to disclose your personal data to us (your "**authorised representative**", which may include your job placement agent), after (i) you (or your authorised representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your personal data for those purposes, or (b) collection and use of personal data without consent is permitted or required by the PDPA or other laws. We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law).

6. Your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes:

(a) performing obligations under or in connection with your contract of employment with us, including payment of remuneration and tax;
(b) all administrative and human resources related matters within our organisation, including administering payroll, granting access to our premises and computer systems, processing leave applications, administering your insurance and other benefits, processing your claims and expenses, investigating any acts or defaults (or suspected acts or defaults) and developing human resource policies;
(c) managing and terminating our employment relationship with you, including monitoring your internet access and your use of

our intranet email to investigate potential contraventions of our internal or external compliance regulations, and resolving any employment related grievances;

(d) assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position within our organisation;

(e) ensuring business continuity for our organisation in the event that your employment with us is or will be terminated;

(f) performing obligations under or in connection with the provision of our goods or services to our clients;

(g) facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of our organisation, or corporate restructuring process; and

(h) facilitating our compliance with any laws, customs and regulations which may be applicable to us.

7. The purposes listed in the above clauses may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under any contract with you).

RELIANCE ON LEGITIMATE INTERESTS EXCEPTION

8. In compliance with the PDPA, we may collect, use or disclose your personal data without your consent for the legitimate interests of Digipixel or another person. In relying on the legitimate interests exception of the PDPA, Digipixel will assess the likely adverse effects on the individual and determine that the legitimate interests outweigh any adverse effect.

9. In line with the legitimate interests' exception, we will collect, use or disclose your personal data for the following purposes:

(a) Fraud detection and prevention;

(b) Detection and prevention of misuse of services;

(c) Network analysis to prevent fraud and financial crime, and perform credit analysis; and

(d) Collection and use of personal data on company-issued devices to prevent data loss.

The purposes listed in the above clause may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter.

WITHDRAWING YOUR CONSENT

10. The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. You may withdraw consent and request us to stop collecting, using and/or disclosing your personal data by submitting your request in writing or via email to our Data Protection Officer at the contact details provided below. Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.

11. Upon receipt of your written request to withdraw your consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process your request within fourteen (14) business days of receiving it.

ACCESS TO AND CORRECTION OF PERSONAL DATA

12. If you wish to make (a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or (b) a correction request to correct or update any of your personal data which we hold, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.
13. Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request.

14. We will respond to your request as soon as reasonably possible. In general, our response will be within seven (7) business days. Should we not be able to respond to your access request within fourteen (14) days after receiving your access request, we will inform you in writing within fourteen (14) days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA).

15. Please note that depending on the request that is being made, we will only need to provide you with access to the personal data contained in the documents requested, and not to the entire documents themselves. In those cases, it may be appropriate for us to simply provide you with confirmation of the personal data that our organisation has on record, if the record of your personal data forms a negligible part of the document.

PROTECTION OF PERSONAL DATA

16. To safeguard your personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as minimised collection of personal data, authentication and access controls (such as good password practices, need-to-basis for data disclosure, etc.), encryption of data, data anonymisation, up-to-date antivirus protection, regular patching of operating system and other software, securely erase storage media in devices before disposal, web security measures against risks, usage of one time password(otp)/2 factor authentication (2fa)/multi-factor authentication (mfa) to secure access, security review and testing performed regularly, credential exposure checks, device vulnerability assessments and security hardening.

17. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

ACCURACY OF PERSONAL DATA

18. We generally rely on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

RETENTION OF PERSONAL DATA

19. We may retain your personal data for as long as it is necessary to fulfil the purposes for which they were collected, or as required or permitted by applicable laws.

20. We will cease to retain your personal data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the personal data were collected, and are no longer necessary for legal or business purposes.

TRANSFERS OF PERSONAL DATA OUTSIDE OF SINGAPORE

21. We generally rely on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

DATA PROTECTION OFFICER

22. You may contact our Data Protection Officer if you have any enquiries or feedback on our personal data protection policies and procedures; or if you wish to make any request, in the following manner:

    Name of DPO : Mr. Dave Gurbani
    Contact No. : +65 8725 9789
    Email Address : dpo@cybersafe.sg

EFFECT OF NOTICE AND CHANGES TO NOTICE

23. This Notice applies in conjunction with any other policies, notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

24. We may revise this Notice from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued employment and participation in our recruitment process constitute your acknowledgement and acceptance of such changes.

    Effective date : 15/01/2024
    Last updated : 15/01/2024

4.1.2 Job Applicants

This Data Protection Notice ("**Notice**") sets out the basis upon which Digipixel ("**we**", "**us**", or "**our**") may collect, use, disclose or otherwise process personal data of job applicants in accordance with the Personal Data Protection Act ("**PDPA**"). This Policy applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.

APPLICATION OF THIS NOTICE

1. This Notice applies to all persons who have applied for any such position with us ("**job applicants**").

PERSONAL DATA

2. As used in this Notice, "**personal data**" means data, whether true or not, about an employee or a job applicant who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

3. Personal data which we may collect includes, without limitation, your:

(a) name or alias, gender, last 4 characters of you NRIC/FIN or passport number, date of birth, nationality, and country of birth;
(b) mailing address, telephone numbers, email address and other contact details;
(c) resume, educational qualifications, professional qualifications and certifications and employment references;
(d) employment and training history;
(e) salary information and bank account details;
(f) details of your next-of-kin, spouse and other family members;
(g) work-related health issues and disabilities; and
(h) photographs.

4. Other terms used in this Notice shall have the meanings given to them in the PDPA (where the context so permits).

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

5. We generally collect personal data that (a) you knowingly and voluntarily provide in the course of or in connection with your employment or job application with us, or via a third party who has been duly authorised by you to disclose your personal data to us (your "**authorised representative**", which may include your job placement agent), after (i) you (or your authorised representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your personal data for those purposes, or (b) collection and use of personal data without consent is permitted or required by the PDPA or other laws. We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law).

6. Your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes:

(a) assessing and evaluating your suitability for employment in any current or prospective position within the organisation;
(b) verifying your identity and the accuracy of your personal details and other information provided;
(c) performing obligations under or in connection with your contract of employment with us, including payment of remuneration and tax;
(d) all administrative and human resources related matters within our organisation, including administering payroll, granting access to our premises and computer systems, processing leave applications, administering your insurance and other benefits, processing your claims and expenses, investigating any acts or defaults (or suspected acts or defaults) and developing human resource policies;

(e) managing and terminating our employment relationship with you, including monitoring your internet access and your use of our intranet email to investigate potential contraventions of our internal or external compliance regulations, and resolving any employment related grievances;
(f) assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position within our organisation;
(g) ensuring business continuity for our organisation in the event that your employment with us is or will be terminated;
(h) performing obligations under or in connection with the provision of our goods or services to our clients;
(i) facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of our organisation, or corporate restructuring process; and
(j) facilitating our compliance with any laws, customs and regulations which may be applicable to us.

7. The purposes listed in the above clauses may continue to apply even in situations where your relationship with us (for example, pursuant to your employment contract should you be hired) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under a contract with you).

RELIANCE ON LEGITIMATE INTERESTS EXCEPTION

8. In compliance with the PDPA, we may collect, use or disclose your personal data without your consent for the legitimate interests of Digipixel or another person. In relying on the legitimate interests exception of the PDPA, Digipixel will assess the likely adverse effects on the individual and determine that the legitimate interests outweigh any adverse effect.

9. In line with the legitimate interests' exception, we will collect, use or disclose your personal data for the following purposes:

(a) Fraud detection and prevention;
(b) Detection and prevention of misuse of services;
(c) Network analysis to prevent fraud and financial crime, and perform credit analysis; and
(d) Collection and use of personal data on company-issued devices to prevent data loss.

The purposes listed in the above clause may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter.

WITHDRAWING YOUR CONSENT

10. The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. As a job applicant, you may withdraw consent and request us to stop collecting, using and/or disclosing your personal data for any or all of the purposes listed above by submitting your request in writing or via email to our Data Protection Officer at the contact details provided below.

11. Upon receipt of your written request to withdraw your consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process and effect your request within fourteen (14) days of receiving it.

12. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and extent of your request, we may not be in a position to process your job application (as the case may be). We shall, in such circumstances, notify you before completing the processing of your request (as outlined above). Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in clause 8 above.

13. Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.

ACCESS TO AND CORRECTION OF PERSONAL DATA

14. If you wish to make (a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or (b) a correction request to correct or update any of your personal data which we hold, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.

15. Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request.

16. We will respond to your request as soon as reasonably possible. In general, our response will be within seven (7) business days. Should we not be able to respond to your access request within fourteen (14) days after receiving your access request, we will inform you in writing

within fourteen (14) days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA).

17. Please note that depending on the request that is being made, we will only need to provide you with access to the personal data contained in the documents requested, and not to the entire documents themselves. In those cases, it may be appropriate for us to simply provide you with confirmation of the personal data that our organisation has on record, if the record of your personal data forms a negligible part of the document.

PROTECTION OF PERSONAL DATA

18. To safeguard your personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as minimised collection of personal data, authentication and access controls (such as good password practices, need-to-basis for data disclosure, etc.), encryption of data, data anonymisation, up-to-date antivirus protection, regular patching of operating system and other software, securely erase storage media in devices before disposal, web security measures against risks, usage of one time password(otp)/2 factor authentication (2fa)/multi-factor authentication (mfa) to secure access, security review and testing performed regularly, credential exposure checks, device vulnerability assessments and security hardening.

19. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

ACCURACY OF PERSONAL DATA

20. We generally rely on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

RETENTION OF PERSONAL DATA

21. We may retain your personal data for as long as it is necessary to fulfil the purposes for which they were collected, or as required or permitted by applicable laws.

22. We will cease to retain your personal data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the personal data were collected, and are no longer necessary for legal or business purposes.

TRANSFERS OF PERSONAL DATA OUTSIDE OF SINGAPORE

23. We generally do not transfer your personal data to countries outside of Singapore. However, if we do so, we will obtain your consent for the transfer to be made and will take steps to ensure that your personal data continues to receive a standard of protection that is at least comparable to that provided under the PDPA.

DATA PROTECTION OFFICER

24. You may contact our Data Protection Officer if you have any enquiries or feedback on our personal data protection policies and procedures; or if you wish to make any request, in the following manner:

Name of DPO : Mr. Dave Gurbani
Contact No. : +65 8725 9789
Email Address : dpo@cybersafe.sg

EFFECT OF NOTICE AND CHANGES OF NOTICE

25. This Notice applies in conjunction with any other policies, notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

26. We may revise this Notice from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued employment and participation in our recruitment process constitute your acknowledgement and acceptance of such changes.

Effective date : 15/01/2024
Last updated : 15/01/2024

4.1.3 Customers

This Data Protection Notice ("Notice") sets out the basis which Digipixel ("**we**", "**us**", or "**our**") may collect, use, disclose or otherwise process personal data of our customers in accordance with the Personal Data Protection Act ("**PDPA**"). This Notice applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.

Here at Digipixel, we take just as much pride in providing you with data protection. This notice is to inform you on our adherence to the obligations of the PDPA as well as the steps we have taken to provide security and protection for the data you have provided. This notice will also be taken as deemed consent unless otherwise stated.

PERSONAL DATA

1. As used in this Notice:

   "**customer**" means an individual who (a) has contacted us through any means to find out more about any goods or services we provide, or (b) may, or has, entered into a contract with us for the supply of any goods or services by us; and

   "**personal data**" means data, whether true or not, about a customer who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

2. Depending on the nature of your interaction with us, some examples of personal data which we may collect from you include name, residential address, email address, telephone number, nationality, gender, date of birth, marital status, photograph, employment information and financial information.

3. Other terms used in this Notice shall have the meanings given to them in the PDPA (where the context so permits).

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

4. We generally do not collect your personal data unless (a) it is provided to us voluntarily by you directly or via a third party who has been duly authorised by you to disclose your personal data to us (your "**authorised representative**") after (i) you (or your authorised representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your personal data for those purposes, or (b) collection and use of personal data without consent is permitted or required by the PDPA or other laws. We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law).

5. We may collect and use your personal data for any or all of the following purposes:

   (a) performing obligations in the course of or in connection with our provision of the goods and/or services requested by you;
   (b) verifying your identity;

(c) responding to, handling, and processing queries, requests, applications, complaints, and feedback from you;
(d) managing your relationship with us;
(e) processing payment or credit transactions;
(f) complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority;
(g) any other purposes for which you have provided the information;
(h) transmitting to any unaffiliated third parties including our third party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes;
(i) any other incidental business purposes related to or in connection with the above; and
(j) website visitor traffic and informatics via cookies stored on our website, -Organisation's Website URL-.

6. We may disclose your personal data:

(a) where such disclosure is required for performing obligations in the course of or in connection with our provision of the goods and services requested by you;
(b) to third party service providers, agents and other organisations we have engaged to perform any of the functions with reference to the above mentioned purposes; or
(c) complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority.

7. The purposes listed in the above clauses may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under a contract with you).

RELIANCE ON THE LEGITIMATE INTERESTS EXCEPTION

8. In compliance with the PDPA, we may collect, use or disclose your personal data without your consent for the legitimate interests of Digipixel or another person. In relying on the legitimate interests exception of the PDPA, Digipixel will assess the likely adverse effects on the individual and determine that the legitimate interests outweigh any adverse effect.

9. In line with the legitimate interests' exception, we will collect, use or disclose your personal data for the following purposes:

(a) Fraud detection and prevention;
(b) Detection and prevention of misuse of services;
(c) Network analysis to prevent fraud and financial crime, and perform credit analysis; and
(d) Collection and use of personal data on company-issued devices to prevent data loss.

The purposes listed in the above clause may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter.

WITHDRAWING YOUR CONSENT

10. The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. You may withdraw consent and request us to stop collecting, using and/or disclosing your personal data for any or all of the purposes listed above by submitting your request in writing or via email to our Data Protection Officer at the contact details provided below.

11. Upon receipt of your written request to withdraw your consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process your request within fourteen (14) business days of receiving it.

12. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and scope of your request, we may not be in a position to continue providing our goods or services to you and we shall, in such circumstances, notify you before completing the processing of your request. Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in clause 8 above.

13. Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.

ACCESS TO AND CORRECTION OF PERSONAL DATA

14. If you wish to make (a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or (b) a correction request to correct or update any of your personal data which we hold

about you, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.

15. Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request.

16. We will respond to your request as soon as reasonably possible. In general, our response will be within seven (7) business days. Should we not be able to respond to your request within fourteen (14) days after receiving your request, we will inform you in writing within fourteen (14) days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA).

PROTECTION OF PERSONAL DATA

17. To safeguard your personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as minimised collection of personal data, authentication and access controls (such as good password practices, need-to-basis for data disclosure, etc.), encryption of data, data anonymisation, up-to-date antivirus protection, regular patching of operating system and other software, securely erase storage media in devices before disposal, web security measures against risks, usage of one time password(otp)/2 factor authentication (2fa)/multi-factor authentication (mfa) to secure access, security review and testing performed regularly, credential exposure checks, device vulnerability assessments and security hardening.

18. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

ACCURACY OF PERSONAL DATA

19. We generally rely on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

RETENTION OF PERSONAL DATA

20. We may retain your personal data for as long as it is necessary to fulfil the purpose for which it was collected, or as required or permitted by applicable laws.

21. We will cease to retain your personal data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purpose for which the personal data was collected, and is no longer necessary for legal or business purposes.

TRANSFERS OF PERSONAL DATA OUTSIDE OF SINGAPORE

22. We generally do not transfer your personal data to countries outside of Singapore. However, if we do so, we will obtain your consent for the transfer to be made and we will take steps to ensure that your personal data continues to receive a standard of protection that is at least comparable to that provided under the PDPA.

WEBSITE

23. Our website, Digipixel, may contain links to other sites; These sites do not operate under the Policy set forth for our company and website. You are advised to review the policies displayed in those websites before use.

24. Our websites do contain cookies. These cookies improve the overall experience you have visiting our site and provide us with informatics on how we can better serve you and improve your user experience.

25. We retain the copyrights to the material including logo, photographs and content found on these sites. No part of these websites may be copied, performed in public, utilised and/or adapted without our written consent

DATA PROTECTION OFFICER

26. You may contact our Data Protection Officer if you have any enquiries or feedback on our personal data protection policies and procedures, or if you wish to make any request, in the following manner:

Name of DPO	: Mr. Dave Gurbani
Contact No.	: +65 8725 9789
Email Address	: dpo@cybersafe.sg

EFFECT OF NOTICE AND CHANGES TO NOTICE

27. This Notice applies in conjunction with any other notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

28. We may revise this Notice from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued use of our services constitutes your acknowledgement and acceptance of such changes.

Effective date : 15/01/2024
Last updated : 15/01/2024

4.2 Security

4.2.1 Access Control

4.2.1.1 **Overview –** Active user accounts and physical access are the source of entry to the hardware and software in the enterprise environment. Ensuring that only authorised users are given the access rights they need to perform their work helps reduce the risk of information being stolen, or hardware and software being compromised.

4.2.1.2 **Purpose –** The purpose is to ensure that access controls are implemented and to protect the sources of entry to the hardware and software in the enterprise environment.

4.2.1.3 **Scope –** This policy or guideline applies to all employees and third parties, including suppliers who have access to the organisation's systems, data, and resources.

4.2.1.4 **Roles and Responsibilities –** The roles and responsibilities of employees involved in carrying out and maintaining access controls:

1. Requestor: End users
2. Approver: Tan Yong Li
3. Administrator: Tan Yong Li (yongli@digipixel.sg), Islam MD Tarccqul (tareq@digipixel.sg)

4.2.1.5 **Principle of least privilege –** Access control is assigned on the basis of business needs and 'Least Privilege'. Users must only be provided with the absolute minimum access rights and permissions to systems, data, and resources that they need to fulfil their job roles.

4.2.1.6 **User access account management –** User account management procedures must be implemented for the following:

1. Account creation, modification, and deletion
2. Account monitoring:
   - Ensure there are no shared, duplicate, obsolete, or invalid accounts.
   - Ensure dormant or accounts that have been inactive for a prolonged period [30 days] are removed or disabled.
   - Removal of accounts with access rights that are no longer required or have exceeded the requested date.
3. Use of administrator accounts – Limited to performing administrator functions, with approval from senior management Tan Yong Li (yongli@digipixel.sg)
4. Account locking or disabling after [10] failed login attempts.
5. Login attempts – Will be disable using Google Workspace admin security settings: No login allowed without 2FA enrolment and Trusted Device authentication – Zero Trust. Zero attempts allowed without 2FA.
6. Logging of:

- All creation, modification, and deletion of system and user access
- Login attempts.

7. Regular reviews of system and user access

4.2.1.7 **Process for granting and revoking of access –** The process to request to grant and revoke access includes the following:

1. Requestor ensures the need for access to be granted/revoked and sends in a request, providing:
   - Name and department of employee.
   - System to access.
   - Role/account type requested.
   - Duration for access.
2. Approver to review the request.
3. If the request is approved, Administrator to grant/revoke access accordingly.
4. Administrator to notify the requestor on the access changes for confirmation.

4.2.1.8 **Process to request for administrative access to system –** The process to request to grant and revoke access includes the following:

1. Requestor ensures that administrative access is required and sends in a request.
2. Approver to review the request.
3. If the request is approved, Administrator to create the account and notify the requestor.
4. Administrator to notify the requestor on the access changes for confirmation.

4.2.1.9 **Process for granting and revoking of physical access –** The process to request to grant and revoke physical access to assets includes the following:

1. Requestor ensures that physical access has to be granted/revoked and sends in a request.
2. Approver to review the request.
3. If the request is approved, Administrator to grant/revoke access accordingly.
4. Administrator to notify the requestor on access changes for confirmation.
5. Administrator to notify the physical access control team.

4.2.2 Asset Management

4.2.2.1 **Overview –** Cybersecurity asset management is the process of identifying, continuously, the hardware and software in the organisation to identify the potential security risks. It is needed to ensure that the assets are (i) authorised to access the enterprise environment, and (ii) secured properly to reduce the total cost of risks related to asset management.

4.2.2.2 **Purpose –** The purpose is to protect organisation assets by preventing unauthorised disclosure, modification, removal, or destruction of information assets that may lead to interruptions in business activities.

4.2.2.3 **Scope –** This policy or guideline applies to all parties operating within the organisation environment, and all the assets owned by the organisation.

4.2.2.4 **Roles and Responsibilities –** The roles and responsibilities of employees who are involved in asset management include:

1. Asset manager : Dave Gurbani (dave@cybersafe.sg)
2. End users

4.2.2.5 **Asset Management Lifecycle –** The asset management lifecycle comprises the infrastructure and processes necessary for the effective management, control, and protection of the assets within the organisation, throughout its lifecycle.

1. Planning:
   - Establish the requirement of an asset.
   - Identify the need for the asset.
2. Get approval/authorisation from Tan Yong Li (yongli@digipixel.sg) for the procurement of the asset.
3. Procurement:
   - Ensure assets procured are as per the required specification.
   - Check status of assets and update the relevant inventory.
4. Onboarding:
   - Ensure checks are being done before onboarding assets into the organisation's environment.
   - Seek approval from Tan Yong Li (yongli@digipixel.sg) to onboard new assets.
   - Update inventory once assets are onboarded.
5. Monitoring and Maintenance:
   - Monitor assets periodically and check for any performance issues that could unexpectedly develop, e.g. monitor End-of-Life (EOL) and End-of -Support (EOS).
   - Conduct yearly asset audit to assess assets.
   - Perform periodic maintenance to ensure that all assets are maintained.
6. Disposal:
   - Assets shall be disposed of after EOL/EOS.
   - If the organisation intends to continue using an EOS asset, assess the risk and obtain approval from Dave Gurbani (dave@cybersafe.sg) .Actively monitor the EOS asset until it is replaced.
7. Assets containing information valued as critical and vital shall be disposed of securely and safely. All confidential information shall be

deleted prior to disposal, and the asset disposed of securely and completely.

4.2.3 Data Backup

4.2.3.1 **Overview – –** Data backups are critical in enabling quick recovery from cyber security incidents such as ransomware or malware, but also physical incidents such as system failure, theft, or natural disasters.

4.2.3.2 **Purpose –** The purpose is to create a backup plan that allows the business to continue its operation after a system failure or incident.

4.2.3.3 **Scope –** The policy or guideline includes all types of media format (e.g. hard disk, magnetic tape), data, and personnel.

4.2.3.4 **Roles and Responsibilities –** The roles and responsibilities of the employees involved in carrying out, maintaining, and restoring a data backup:

1. Backup manager: Dave Gurbani (dave@cybersafe.sg)
2. End users

4.2.3.5 **Types of Backups**

- **Full backup –** The complete data is backed up and stored, and as such it requires the most space and time to complete — but is restored in the shortest time. Used for completeness of data.
- **Differential backup –** Performs backup faster and requires less space than a full backup, but performs backup slower than an incremental backup, and slower restoration than a full backup. Used when downtime and cost need to be minimised.
- **Incremental backup –** Perform the fastest backup with the least amount of space required, but with the slowest restoration time compared to a full and differential backup. Used when backup speed is of top priority and where site-to-site backup is limited.

4.2.3.6 **Backup Schedule**

[Type of data, e.g. more critical data]

- Frequency: [Monthly]
- Type of backup: [Full Backup, C2C]

[Type of data, e.g. less critical data]

- Frequency: [Weekly]
- Type of backup: [Full Backup, C2C]

4.2.3.7 **Backup Storage, Retention and Destruction**

- Backup data and logs should be:

    - Stored securely, and protected from unauthorised access through physical and logical security controls.
    - Retained for at least [3 years].
- Deleted securely to purge off the data completely and with secure destruction carried out when no longer needed.
- Backup of critical-business data should be stored offsite.

4.2.3.8 **Backup Recovery Test**

- Data recovery testing should be performed.
- The frequency, testing procedures, and the testing outcomes should be documented and reported to senior management.
- Steps to be carried out by the personnel in data backup and restoration should be clearly documented for testing with improvement points that can used to update the data backup policy.

4.2.4 Configuration Management

4.2.4.1 **Overview –** Configuration management is the process of managing the configurable components or resources of a system or environment on which a software application runs to ensure these resources and components maintain a consistent, or baseline, state. It is important to ensure the organisation has visibility over the secure configuration of its assets and maintains effective control of its IT systems.

4.2.4.2 **Purpose –** The purpose is to ensure the assets in the organisation are being configured securely against a baseline that is compliant with the IT security policies, standards, and procedures.

4.2.4.3 **Scope –** It includes both hardware (e.g. network devices, end points, mobile devices) and software (e.g. anti-virus) that are configurable and that pose a threat to the organisation's production environment if compromised.

4.2.4.4 **Roles and Responsibilities –** The roles and responsibilities of employees involved in configuration management:

1. Configuration management sponsor: Dave Gurbani (dave@cybersafe.sg)
2. Configuration manager: Dave Gurbani (dave@cybersafe.sg)

4.2.4.5 **Security Baseline Configuration –**

1. The assets should be configured and secured based on widely accepted and well-established security standards and benchmarks.
    - Avoid or update weak or default configurations.
2. Replace or upgrade insecure configurations and weak protocols.
3. Reviews should be regularly carried out to update the configuration.
4. Retain the previous configuration as a form of contingency. The configurations and security standards referenced should also be tracked and documented as part of an asset configuration list.

5. Disable or remove features, services, or applications that are not in use.
    - Disable automatic connection to open networks and the auto-run feature of non-essential programs.

4.2.4.6 **Configuration Change Control –** Changes in configuration to assets shall be reviewed and approved by authorised personnel with the relevant change documents, risk assessment, impact analysis and contingency plan which have been tested and verified before deployment to the production environment.

4.2.4.7 **Logging –** Logging should be enabled by default and saved to a central repository that is kept secure against unauthorised access to assist in carrying out diagnosis, troubleshooting or reconciliation of events.

4.2.4.8 **Conformity to configuration standards –** Put in place a process to ensure that the systems in scope conform to the security baseline configuration. Any deviation or non-conformance should be reviewed, monitored, approved, and reported to the senior management with sufficient mitigating controls in place. Employees who violate this policy may also be subjected to disciplinary actions.

4.2.5 Data Management

4.2.5.1 **Overview –** Data is the enterprise's most valuable business asset. Identifying the critical data in the enterprise is the key foundational step to classify, monitor, and protect it to ensure that only authorised personnel can access it.

4.2.5.2 **Purpose –** The purpose is to classify data based on its sensitivity, value, and impact as the result of a compromise to the organisation, so that sufficient measures can be carried out to protect them.

4.2.5.3 **Scope –** This policy or guideline applies to all parties operating within the organisation environment, and all the business-critical data assets owned by the organisation.

4.2.5.4 **Roles and Responsibilities –** The roles and responsibilities of the employees involved in carrying out and maintaining the data classification:

1. Data owner: Tan Yong Li (yongli@digipixel.sg)
2. Data custodian: Tan Yong Li (yongli@digipixel.sg)

4.2.5.5 **Data Classification –** The procedures to carry out data classification, based on the sensitivity level and overall business impact to the organisation.

4.2.5.6 **Data Protection and Handling –** The following data protection and handling measures that are in place include:

- Protection of business-critical data through [password protection | encryption of data]
- Secure deletion of data from media before secure disposal
- Shredding of paper-based data (hard copy) before secure disposal

4.2.5.7 **Data Loss Prevention –** The following data loss prevention measures and controls that are in place to restrict the leakage and loss of confidential and/or sensitive data include:

- Disabling USB drives and enforcing policies on the use of external disks.
- Imposing guidelines that should be adhered to by all the employees, e.g. Not sending any company information to private email address.
- All users Google Workspace drive shared folders will not be given permission to delete folders, files and documents.

4.2.5.8 **Reporting of data breach and compromise –** Suspected data breaches and compromise within the organisation should be reported to: Dave Gurbani (dpo@cybersafe.sg)

4.2.6 IT Acceptable Use Policy

4.2.6.1 **Overview –** The IT Acceptable Use Policy serves to govern and protect the IT resources and equipment in the organisation to minimise risks and damages as a result of improper or insecure usage.

4.2.6.2 **Purpose –** The purpose of this policy is to establish a framework consisting of the rules and guidelines to govern the organisation's IT resources through proper and secure usage of the IT resources in the organisation.

4.2.6.3 **Scope –** This policy applies to all employees and suppliers who have access to the organisation's IT resources. The scope of the IT resources includes hardware and software connected to and accessed through the organisation's network, e.g. printers, emails, mobile devices, etc.

4.2.6.4 **General –** General guidelines and rules of the Dos and Don'ts, e.g. do not engage in unlawful activities, tamper with the IT resources, etc.

4.2.6.5 **Hardware –** Specific guidelines and rules of the Dos and Don'ts when using and handling any in-scope hardware systems, e.g.

- Do connect corporate devices to only trusted network connections when using them to access organisation data.
- Do not leave your corporate devices unattended and unlocked.
- Attach only approved USB devices to corporate devices.

4.2.6.6 **Software –** Specific guidelines and rules of the Dos and Don'ts when using and handling any in-scope software and applications, e.g.

- Do not open email attachments or files downloaded from untrusted or unverified sources.

- Do check that the software is licensed and supported by updates.

4.2.6.7 **Reporting of violation and security events –** The user's responsibilities in reporting any violations of the policy, or suspected security events, and in taking the necessary corrective actions.

4.2.6.8 **Review Schedule –** The frequency of when the policy should be reviewed and signed off with the version, date, and signature by senior management.

4.2.7 Passphrase Management

4.2.7.1 **Overview –** A strong passphrase provides the first line of defence against unauthorised access to the organisation's system, network, or data. A stronger passphrase provides better protection from hackers and malicious software.

4.2.7.2 **Purpose –** The purpose is to establish standards and guiding principles for setting strong passphrases.

4.2.7.3 **Scope –** This policy or guideline applies to all the accounts (e.g. service or privileged account) of systems and networks in the organisation.

4.2.7.4 **General Guidelines –** All systems-level passphrases (e.g. root, administrator accounts) must be changed at least every [90] days. All user-level passphrases (e.g. email, web) must be changed at least every [90] days, and the past [10] passphrases shall not be re-used.

4.2.7.5 **Passphrase Requirement –** All passphrases must conform to the prescribed guidelines.

No.	Strong passphrase guiding principles	Explanation
1	Passphrase is at least twelve characters long	Having a longer passphrase is typically more secure than a complex passphrase as they are harder to brute force. Based on industry best practices and guidelines for security standards on password policy, it is recommended for passphrases to be at least twelve characters long.
2	Passphrase is mixed with upper case, lower case, numbers, and/or special characters	Having a complex passphrase can help to further increase the strength of a passphrase by expanding the possible combination. The passphrase can consist of upper case and lower-case letters, numbers and/or special characters in any order.
3	Passphrase is made up of five random words that are easy to remember	A passphrase consisting of around five random words serves the same function to increase the strength of the passphrase by making it long and unpredictable, yet easy to remember.
4	Passphrase is unpredictable	Using a default or predictable passphrase makes it easier for attackers to crack it by brute force. For

		example, one of the most commonly used passwords, '111111', has been used over 13 million times in 2021.
5	Passphrase is unique for different accounts	Using a passphrase that is unique across every account would mean that in the event of a passphrase compromise, the other accounts belonging to the same user would not be exposed to the risks, as compared to if they were all using the same passphrase. The trade-off is that the user would need to remember which passphrase was used for each account.
7	Passphrase need not be changed frequently unless it has been, or is suspected of being, compromised	Excessive changing of passphrases can bring more harm than good, as users would constantly be forced to come up with new passphrases. They would also be more likely to come up with a predictable passphrase based on their old passphrase, e.g. increase the number sequentially from "password1" to "password2". The trade-off is that an employee's passphrase that has been compromised unknowingly can be used by cyber attackers for a prolonged period of time without anyone noticing.

4.2.7.6 **Passphrase Protection –** Passphrases must be protected from unauthorised disclosure, stored securely, and prevented from being transmitted in the open.

Passphrases should not be:

- Revealed to anyone, or on questionnaires or forms.
- Written down and stored in an open area.
- Stored in an unprotected file on computer system.

4.2.7.7 **Passphrase Change**

1. The passphrase needs to be changed and updated under these circumstances to ensure that access to user accounts is not being compromised.
2. Immediately after installation, all default system and vendor passwords must be changed.
3. In the event of any suspected compromise, the account passphrases shall be changed.

4.2.8 Software Patch Management

4.2.8.1 **Overview –** Software patch management is the process of distributing and applying updates to software. These patches are necessary to update, fix, or enhance the software, including fixing security vulnerabilities, as well as protecting software and operating systems from exploitation.

4.2.8.2 **Purpose –** The purpose is to secure the organisation by ensuring an appropriate patch management policy is in place.

4.2.8.3 **Scope –** This policy or guideline applies to all hardware and software used in the organisation's systems.

4.2.8.4 **Roles and Responsibilities –** The roles and responsibilities of the employees involved in patch management:

1. Patch manager: Dave Gurbani (dpo@cybersafe.sg)
2. End users

4.2.8.5 **Patch Management Process –** The patch management process includes the following:

1. Visiting official sources for vulnerabilities, patches, and updates.
2. Maintaining an up-to-date inventory of hardware and software assets to allow tracking of the latest patches.
3. Testing of patches. This would be done in a test environment before roll out to ensure that the production environment is not affected after the patch. For smaller organisations, it would be recommended to test the patches on the least critical servers that could be easily recovered in case of a system failure.
4. Developing and implementing a patch schedule which includes automated and manual patching to ensure all patches are applied regularly and timely.
5. Monitoring of patches deployed to ensure that that there is no repercussion and the system or device patched is still functioning as it was before.

5 DATA CLASSIFICATION

Data classes:	Class 1 — Restricted	Class 2 — Confidential	Class 3 — Internal	Class 4 — Public
Definition	Highly sensitive business data that are protected by law, used to identify a person, and if compromised, would put the organisation at significant financial risk	Sensitive data that is only available for use by authorised employees and if compromised, would affect the operations of the organisation negatively	Data that is only available to all employees and not meant for public disclosure	Data that falls within the public domain and is freely available to everyone within and beyond the organisation
Impact of loss	Severe business disruption, loss of reputation, public backlash, and legal implications	Moderate loss of reputation, public backlash, and public gaining knowledge of the organisation's internal processes	Low to medium business disruption	Little to no business impact
Examples	Employee's record, Personal Identifiable Information, financial statements, medical records, contracts	Business plans and business strategy documents, network diagrams, application source codes	Company announcements, newsletters, organisation charts	Website information, press releases, marketing materials, contact information

6 SYSTEM AND NETWORK DIAGRAM

[See Annex B]

7 ASSET INVENTORY MAP

[See Annex C]

8 MANAGING ACCESS & CORRECTION REQUESTS

[See Annex D and E]

9 NON-DISCLOSURE AGREEMENT

[See Annex F]

10 ACCOUNT INVENTORY

[See Annex G]

11 INCIDENT RESPONSE PLAN

[See Annex H]

12 DATA BREACH MANAGEMENT PLAN

[See Annex I]

13 USEFUL LINKS

- PDPC - Guide to Developing Data Protection Management Programme (DPMP)
- PDPC - Guide on Managing and Notifying Data Breaches
- PDPC - PDPA Assessment Tool for Organisations (PATO)
- PDPC - PDPA E-Learning Programme
- PDPC - Data Protection Notice Generator

ANNEX A	POLICY TEMPLATE FOR CUSTOMERS, EMPLOYEES AND JOB APPLICANTS	Customers Employees Job Applicants
ANNEX B	SYSTEM AND NETWORK DIAGRAM	Link
ANNEX C	ASSET INVENTORY MAP	Link
ANNEX D	ACCESS REQUEST FORM	Link
ANNEX E	CORRECTION REQUEST FORM	Link
ANNEX F	NON-DISCLOSURE AGREEMENT	Link

ANNEX G	ACCOUNT INVENTORY	Link
ANNEX H	INCIDENT RESPONSE PLAN	Link
ANNEX I	DATA BREACH MANAGEMENT PLAN	Link