|  |  |
| --- | --- |
| TO |  |
| subject | Due Diligence Framework for Third Parties |

Thank you for assisting ACC to complete its due diligence requirements.

ACC is seeking information from suppliers that demonstrates good and safe practices when dealing with data held at third parties.

Please answer the below questions.

|  |
| --- |
| **PART 1: GOVERNANCE AND TECHNOLOGY OVERVIEW** |
|  | How is security governed in your organisation, presuming the organisation head has the overall responsibility – who else is delegated to implement security; and who manages security risks? |  |
|  | Do you have an information security policy? If so what standards have been used, incorporated or have it based upon – e.g.:AS/NZS ISO/IEC 27002 and/or 27001PSR / NZISMHealth Information Security Framework (HISO 10029:1) |  |
|  | Provide details of what systems are used and how they are protected:Claims/case management/ACC staff relatedEmail (including use of Transport Layer Security [TLS])NetworkMS Office or equivalentRemote access (and to what)Any external file transfer systemOther Systems |  |
|  | What types of firewalls do you use to protect your systems:From external access; andFrom internal access? |  |
|  | Do you operate a web server that is exposed to the Internet, and:What information is on that webserver;Who hosts the webserverWhat is the URL of the website(s) hostedWhat authentication credentials are used on the websites? |  |
|  | Who manages each of these systems? (in-house or outsourced to?) |  |
|  | What is the relationship with the suppliers of services? |  |

|  |
| --- |
| **PART 2: USER AUTHENTICATION** |
|  | What are the password standards for access to your systems (should meet New Zealand PSR/NZISM minimum standard) |  |
|  | What user authentication system do you use for internal access to the above systems? |  |
|  | Do you allow remote access to your systems, e.g. for Case Managers making a workplace visit, or working from home; how do you authenticate these users? |  |

|  |
| --- |
| **PART 3: LOGICAL SECURITY** |
|  | Do you operate public ‘kiosks’ which allow limited access onto your network in any way? If so advise if the system has been security tested and if any issues raised have been remediated. |  |
|  | You must be able to prevent access to the systems and data by non-authorised users – how is this achieved? |  |
|  | What security incidents have you had in the last two years and what has been done to correct the issue(s)?(System Related and seriousness) |  |
|  | Clarify who is responsible for your logical security (Authentication, Access Control, User rights etc), including any partner agreements or outsourcing arrangements |  |
|  | Describe logical security controls for each of your data centres and equipment associated with these data centres |  |
|  | Describe your approach/methodology to network security (firewalls, VLANs, intrusion detection etc.) |  |
|  | Describe your methodology for establishing and maintaining logical security, including monitoring and review |  |
|  | What are the processes for ensuring ongoing logical security access to data on desktops, laptops, tablets and smartphones etc. (e.g. security patching/ updating of operating systems, application and databases; data encryption, anti-malware systems including signature updating and reporting of any detected malware)? |  |
|  | Describe what security systems and procedures are in place to minimise the risk of attack by malware, including spam, infection from infected websites, etc. |  |
|  | Do you allow the use of Portable Storage Devices (PSDs) e.g. USB memory sticks on your network, and if so what are the policies and controls on their use (e.g. encryption, limitation on file types that can be uploaded/downloaded etc.)? |  |

|  |
| --- |
| **PART 4: DATA SECURITY** |
|  | What are the physical locations where claim/ACC staff data is stored (including any production, DR, backup, development and pre-production data locations) |  |
|  | How is data stored for your case management/ACC staff related systems? Include answers to where; encrypted or not; access to data processes including protection from unauthorised access? |  |
|  | What are the encryption protocols used if not given above and do these meet NZISM and/or FIPS standards? |  |
|  | What are the rules/processes for archiving data, and are third parties involved, in which case who are they? |  |
|  | What happens when data is no longer required – what are the policies and processes for deletion? |  |
|  | What data is stored on desktop hard drives, laptops or portable storage devices or other media (e.g. CDs) and how is this protected? |  |
|  | What information about ACC clients/staff is stored in hard copy and what security measures are taken to protect this information and prevent unauthorised access to these files, both within the office and during off site meetings? |  |
|  | What are your disaster recovery and business continuity plans to ensure that data is accessible and recoverable? Please attach a copy of your BCP. | . |

|  |
| --- |
| **PART 5: PHYSICAL SECURITY:** |
|  | What are your physical security controls, processes and policies? (include details of physical access control systems – electronic or physical [i.e. keys]) |  |
|  | What procedures are in place for vetting potential new employees? |  |
|  | What is the exit procedure for staff as it relates to security? |  |
|  | What are your procedures for allowing visitors access to your premises or data processing systems and how will you ensure that data provided by ACC remains secure from these visitors access? |  |
|  | Where do you meet with ACC clients/staff (e.g. your offices, their homes/workplaces etc.)? |  |
|  | What are your security policies for meeting with clients/staff (e.g. two staff must be present; an escape door must be available, etc.)? |  |
|  | Do you provide other protective security measures when meeting with clients/staff eg. observable recording by voice and/or CCTV/video recording? |  |
|  | What are your controls and procedures for restricting the transportation of media and/or assets and/or files into and out of your premises? |  |
|  | What are your controls and procedures for disposal of surplus computer equipment including magnetic, optical and non-volatile (e.g. USB memory) storage media? |  |
|  | What are the controls and processes for any off site storage facilities e.g. archived files, backup tapes? |  |

|  |
| --- |
| **PART 6: OTHER** |
|  | Do you, or your IT services supplier, have any applicable accreditation for security? E.g. SSAE 16, ISO/IEC 27001 |  |
|  | What standards do you comply with in relation to the question above? |  |
|  | What audit processes and policies do you have – both internal and external? |  |
|  | When was your last audit and what was the result?(Summary of key findings) |  |
|  | What actions have been taken as a result of this audit? |  |
|  | What are you processes for ensuring that all ACC data (both electronic and printed form) is returned and/or securely destroyed at the end of the engagement |  |
|  | What is your policy about your staff bringing work home and working from home? |  |
|  | What is your web browsing policy for your staff? Do you allow webmail (hotmail, yahoo, gmail, etc.) or access to social networking sites (e.g. facebook, bebo, twitter) |  |
|  | Do you operate wireless connections on/to your secure network? If so what security is applied and what encryption protocols are used. How often the passwords are changed and how long and complex are these passwords? |  |
|  | Please advise your policies for dealing with: * Data at Rest
* Data in Transit
* Data in Use
 |  |
|  | Are any of the applications used to support the processing of ACC claims/relevant to ACC staff, located in a Public, Private, Hybrid or Community Cloud |  |
|  | If any Cloud based solutions are deployed for the management of claims/relevant to ACC staff – please provide a completed DIA GCIO 105 Cloud Questionnaire |  |