**On the 25th May 2018 the Data Protection Act 1998 was superseded by the General Data Protection Regulation. As part of these regulatory** **changes companies dealing with data, as either a Data Controller or a Data Processor are legally required to document its procedures and processes.**

**Considering these changes, I would appreciate you taking a little time to complete the following information either personally or by passing on to a colleague and this will enable Barnsley Premier Leisure to record your comments accordingly**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Company Details:** | | | **Contact Details:** | |
| Organisation Name: | |  | Contact Name: |  |
| Address: | |  | Job Title: |  |
| E-mail: |  |
| Web: | |  | Mobile: |  |
| E-mail: | |  | Telephone: |  |
| Telephone: | |  | Completion Date: |  |
| **Products and Services** | | | | |
| Please briefly describe below the nature of the Products and/or Services currently being provided to Barnsley Premier Leisure: | | | | |
|  | | | | |
| **General Data Protection Regulation Requirements** | | | | |
| DP1. | Can you confirm what steps you are taking to meet the General Data Protection Regulation changes on Data Protection and Data Governance? | |  | |
| DP2. | Do you consider yourselves to be a Data Controller or Data Processor when dealing specifically with Barnsley Premier Leisure data? Can you clarify why you have come to this specific decision? | |  | |
| DP3. | Under the Data Subject’s ‘*Right to be forgotten’* can you confirm what process you have in place should a request come in from us to enable this to happen? | |  | |
| **Access to the Barnsley Premier Leisure Network** | | | | |
| Please state for the delivery of your services what, if any, access you require to the Barnsley Premier Leisure network?  Please explain what security is in place within your environment to ensure this is, and maintains, a secure connection. | | |  | |
| Where will the services be provided from? (please tick):  ☐ UK Mainland ☐ Inside European Economic Area  ☐ Outside European Economic Area | | | How many sites will the services be provided from? (please tick):  ☐ Single Site ☐ Multiple Sites | |
| **Sub-Contractors and/or Agents** | | | | |
| Will your organisation use sub-contractors and/or agents, who are not directly employed by your organisation, in the delivery of the services for Barnsley Premier Leisure?  ☐ Yes ☐ No  If YES, please provide details below: (Please note that sub-contractors/agents may be required to complete an information security assessment).   |  |  |  | | --- | --- | --- | | **Sub-Contractor /Agent Name** | **Relationship Status to Third Party** | **Services to be Provided** | |  |  |  | |  |  |  | |  |  |  | | | | | |
| **Accreditation and Certification** | | | | |
| Please provide details of any information security standards and accreditation that your organisation currently holds (include details of the accrediting body, review and audit dates): | | | | |
|  | | | | |

| **Information Security Questions** | | | | **Supplier Response** |
| --- | --- | --- | --- | --- |
| **Information Security Policy** | | | | |
|  | Do you have a published security policies and procedures, which have been approved by its management? | | |  |
|  | Please select the security areas which are addressed by your organisation’s information security policies and standards: | | |  |
| Acceptable Use | Remote Access/Wireless | IT Security Incident Response |
| Data/System Classification | Third Party Access | Physical Security |
| Network/Perimeter Security | Data Privacy | Access Control |
| Encryption Standards | Anti-Virus | E-mail/Instant Messaging |
| Personnel Security | Clear Desk | Secure Software Development |
| Secure Destruction | Change Management |  |
|  | Is a complete set of your organisation’s security policies available for review? | | |  |
|  | Is there a process for annually reviewing, updating, and revising these policies? | | |  |
| **Data Storage and Processing Location** | | | | |
|  | In the provision of services for Barnsley Premier Leisure will your organisation be storing and processing data? If yes, please state the geographical location of the data storage and processing facilities that will be used. | | |  |
| **Personnel Security** | | | | |
|  | How many staff will be involved in the delivery of services for Barnsley Premier Leisure? | | | ☐ Less than 5 ☐ Less than 10 ☐ More than 10 |
|  | How many of these staff may have access to Barnsley Premier Leisure data, network, systems, and/or applications in the delivery of services? | | | ☐ Less than 5 ☐ Less than 10 ☐ More than 10 |
|  | Do terms and conditions of employment clearly define information security requirements, including non-disclosure provisions for employees and contractors? | | |  |
|  | Are all users (your organisation’s employees, agents, contractors, suppliers and other third parties) required to sign confidentiality agreements? | | |  |
|  | Do you have a screening and vetting process for all users (employees, agents, contractors, suppliers and other third parties). | | |  |
|  | Please explain how you conduct formal information security awareness training for all users (employees, agents, contractors, suppliers and other third parties)? | | |  |
|  | Please explain how you provide guidance to all employees and agents, including contractors and service providers for handling information and equipment? | | |  |
|  | Please explain how your employment changes and termination procedures that ensure assets are returned and access rights removed or adjusted. | | |  |
| **Supply Chain Management** | | | | |
|  | Please explain how you ensure that throughout its supply chain third parties and suppliers of information and communication technology services comply with your organisation’s information security management system (ISMS). | | |  |

| **Information Security Controls** | | |
| --- | --- | --- |
| **Information Security Control** | | **Supplier Response** |
|  | **Physical Controls**  Please explain how you control the physical access to your buildings, rooms and equipment to prevent unauthorised entry and access. |  |
|  | **Inventory of Authorised Devices**  Please explain how you track, control, and prevent unauthorised network access by devices (computers, network components, printers, anything with IP addresses). |  |
|  | **Inventory of Authorised Software**  Please explain how you track, control, and prevent unauthorised installation and execution of software on its computers. |  |
|  | **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**  Please explain how you track, control, prevent and correct security weaknesses in the configurations of the hardware and software of its mobile devices, laptops, workstations, and servers. |  |
|  | **Continuous Vulnerability Assessment and Remediation**  Please explain how you track, control, prevent and correct security vulnerabilities in the configurations of its devices. |  |
|  | **Malware Defences**  Please explain how you detect and prevent installation and execution of malicious software on all its devices. |  |
|  | **Application Software Security**  Please explain how you detect, prevent and correct security weaknesses in the development and acquisition of its software applications. |  |
|  | **Wireless Device Control**  Please explain how you ensure the security of your wireless local area networks (LANS), access points, and wireless client systems. |  |
|  | **Data Recovery Capability**  Please explain how you back up critical information with a proven methodology for timely recovery of it. |  |
|  | **Security Skills Assessment and Appropriate Training to Fill Gaps**  Please explain how you continuously ensure that its workforce is effectively trained and aware of security issues. |  |
|  | **Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**  Please explain how you track, control, prevent and correct security weaknesses in the configurations of your network devices such as firewalls, routers, and switches. |  |
|  | **Limitation and Control of Network Ports, Protocols, and Services**  Please explain how you manage and control the use of ports, protocols, and services on networked devices. |  |
|  | **Controlled Use of Administrative Privileges**  Please explain how you manage, control and review the use, assignment, and configuration of administrative privileges on your computers, networks, and applications. |  |
|  | **Boundary Defence**  Please explain how you manage and control the flow of information transferring between networks of different trust levels. |  |
|  | **Maintenance, Monitoring, and Analysis of Audit Logs**  Please explain how you process for auditing, monitoring, testing, and reviewing to ensure compliance with security policies and standards. |  |
|  | **Controlled Access Based on the Need to Know**  Please explain how you ensure secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information. |  |
|  | **Account Monitoring and Control**  Please explain how you manage and controls system and application accounts. |  |
|  | **Data Loss Prevention**  Please explain how you prevent the loss of data in transmission and storage. |  |
|  | **Incident Response and Management**  Please explain how you respond to any adverse events or threats of adverse events. |  |
|  | **Secure Network Engineering**  Please explain how you build, update, and validate your network infrastructure so that you can properly withstand attacks from advanced threats. |  |
|  | **Penetration Tests and Disaster Recovery Testing**  Please explain how you test and validate your overall security. |  |

| **Information Security Questions** | | **Supplier Response** |
| --- | --- | --- |
| **Patch Management** | | |
|  | Please explain how you apply the latest versions of software, service packs and updates for your equipment and infrastructure with minimal delay. |  |
|  | Please explain your approach to auditing, monitoring, and testing your patch management. |  |
| **Auditing and Compliance** | | |
|  | Please indicate that you are willing to provide evidence to support your responses to this Barnsley Premier Leisure security assessment questionnaire, if requested. |  |
|  | Please confirm that your response to this security assessment questionnaire applies to all sites that your organisation will provide the services from including third party sub-contractors’ and agents’ premises used in the provision of services to Barnsley Premier Leisure. |  |

|  |
| --- |
| **Please use the space below to record any further information security issues and concerns that you wish to bring to the attention of Barnsley Premier Leisure:** |
|  |

Thank you for completing this information security assessment questionnaire.