

Data protection and security due diligence

Introduction

As part of the General Data Protection Regulation (GDPR), data controllers (you our customers) are required to only use processors (Intelliflo in this instance), who can provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

Intelliflo receive a large number of questionnaires each year, however we feel that some of these would not provide sufficient evidence that a data controller was fully managing a critical supplier.

As a result we have taken a standard supplier question set, which takes into account the GPDR and answered this. You can use this as evidence that Intelliflo provide sufficient guarantees that they are meeting their obligations to meet the requirement of the GDPR, and protect the rights of the data subjects whose data you handle.

These questions and answers are our response to version 10.7 of IASME Governance and GDPR question set here

<https://www.iasme.co.uk/wp-content/uploads/2018/01/IASME-governance-and-Cyber-Essentials-questions-booklet-v10.7.pdf>

IASME is a governance framework aimed at the SME space, and is a comprehensive set of questions which enable an organisation to measure and demonstrate their security posture.

Why have you certified to ISO 27001 but answered a question set for IASME?

Because IASME is aimed at the SME space - IASME is structured around a set of questions. However, ISO 27001 is aimed at the enterprise space and is a looser framework.

We certify to ISO 27001 because it is a broader standard than IASME. However we answer the IASME questions because ISO 27001 does not give us a set of questions to answer, the IASME questions are publicly available which means you can read them alongside our answers and this IASME question set is explicitly about GDPR.

When you read our answers you should read these answers alongside the IASME document above, which contains more context.

Your organisation

1. What is your organisation's name?
(for companies: as registered with Companies House)

We are called Intelliflo Limited.

2. What is your organisation's registration number?
(if you have one)

Our company number is 05206315.

3. What is your organisation's address?
(for companies: as registered with Companies House)

Intelliflo's main offices are at Intelliflo Ltd, Third Floor Drapers Court, Kingston Hall Road, Kingston upon Thames, Surrey, KT1 2BQ.

4. What is your main business?

Intelliflo are suppliers of SaaS software for IFAs, financial and mortgage advisers allowing focus on clients not administration.

5. What is your website address?

www.intelligent-office.net is our SaaS platform, www.intelliflo.com is our corporate website, if you use myfpf - this will be at a url you have picked which will be along the lines of yourcompanyname.myfpf.co.uk

6. What is the size of your organisation?
(Based on the EU definitions of Micro (<10 employees, <2m turnover), Small (<50 employees, <10m turnover), Medium (<250 employees, <50m turnover) or Large)

Intelliflo have 150 employees, and a turnover of below 50m Euros - so are a medium sized company.

7. How many staff are home workers?
(Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when travelling.)

Around half of Intelliflo's staff work from home or are in the field.

Scope of assessment

8. Does the scope of this assessment cover your whole organisation?

This covers all operations of Intelliflo Limited.

9. If it is not the whole organisation, then what is the scope description you would like to appear on your certificate and website?

See 8, this covers all operations of Intelliflo Limited.

10. Does your organisation hold or process personal data? (as defined by your country's data protection legislation)

Yes, Intelliflo hold personal data as a data controller, and customer owned personal data as your processor.

11. Have you completed a Data Protection Impact Assessment, or Privacy Impact Assessment in the last 12 months?


Yes, we do these as part of our normal change process. Our various technology, and business change management processes include criteria which can lead to PIAs being produced.

12. Is your usage of personal data subject to the EU GDPR? (If you hold and process personal data about EU citizens, you must comply with the EU GDPR wherever you are located in the world).

Yes, we hold data of EU citizens both as controller for the data we collect, and data of EU citizens as our customers' processor. We are subject to and comply with both the controller and processor aspects of the GDPR.

13. Please describe the geographical locations of your business which are in the scope of this assessment.

Intelliflo have a number of sites, the head office in Kingston upon Thames, and we have two data centres in Woking and Docklands.



- 14. Please describe all equipment which is included in the scope of this assessment (please include details of laptops, computers, servers, mobile phones and tablets). All laptops, computers, servers and mobile devices that can access business data and have access to the internet must be included in the scope of the assessment.**

All IT equipment used by Intelliflo to deliver and support the client platform service are covered in this assessment. This covers all laptops, desktops, mobile computing devices such as phones and tablets, all servers, virtual machines, IaaS, PaaS and SaaS cloud instances Intelliflo operate or are operated upon Intelliflo's behalf.

- 15. Please describe the networks that will be in the scope for this assessment. (such as office network, home offices and firewalls)**

All Office networks both physical and wifi, all data centre networks, and all cloud virtual networks.

- 16. Who is responsible for managing the information systems in the scope of this assessment?**

Our COO Robert Walton is responsible for security and data protection.



Managing security

17. Please provide the name of the board member / director / partner / trustee identified as responsible for information security and data protection?

Our COO Robert Walton is responsible for information security and data protection.

18. Is information security and data protection a standing agenda item for your board meetings?

Yes, there are security and risk items reported monthly in every board pack and this is an ISO 27001 control.

19. Please provide the name and role of the person who has overall responsibility for security in your organisation? This should be a named board member or director.

Our COO Robert Walton is responsible for information security and data protection.

**20. Please provide the name and role of the person who has overall responsibility for data protection in your organisation?
(This should be a named board member or director)**

Our COO Robert Walton is responsible for information security and data protection.

21. How do you ensure that you provide sufficient funding and a suitable number of appropriately skilled staff to develop and maintain good information security?

Intelliflo operate a cross functional technical service architecture group, who are responsibility for information security and data protection. This group are all senior technology staff. All technology and security staff have access to pluralsight or lynda online training courses which means they have access to training courses across the full spectrum of information security.

Information assets

22. Does your organisation have up to date asset registers?

Yes, Intelliflo's asset register is audited as part of its ISO 27001 certified ISMS.

23. Does your asset management track your own and other company's intellectual property within your organisation?

Yes, this is tracked using management tools. Most of our licensing is per CPU or per user, rather than per install.

24. Does your asset register track information assets (ie categories of information) as well as physical assets? An information asset might be a set of data (for example "employee information") which will have a location attached to it (for example "the server in the HR department") and an owner (for example the "HR director")

Yes, our asset register is compliant with ISO 27001 and audited as part of our ISO 27001 ISMS, which requires us to track information assets, alongside physical assets and for all assets to be owned.

25. Do all assets (both physical and information assets) have named owners?

Assets are owned by departments and an individual from within that department. Managers of departments are responsible for assets owned by their department.

26. Is removable media recorded and managed?

Intelliflo implement technical controls to make removable media read only, Intelliflo staff cannot copy company data onto removable media. Intelliflo also have technical controls to keep customer data within Intelliflo data centres.

27. Are all mobile phones and tablets tracked in the asset register, pin or password protected, encrypted and remotely wipeable?

(In order to answer "Yes" to this question, all of the criteria listed must be true. This can be achieved using built-in tools or additional mobile device management software.)

All corporate owned phones and tablets are tracked in the asset register, all are PIN protected, and encrypted. They are not remotely wipe-able.

28. Is all personal data and special category data identified (e.g. by protective marking) and properly protected?

(Describe how this is done.)

Intelliflo owned personal data is only stored within Intelliflo contracted SaaS systems, such as Salesforce and Netsuite. Your clients personal data is stored within the iO platform. We have business rules specifying what data is stored where. Data within these platforms is protected with strong technical controls, access to SaaS systems such as Netsuite and Salesforce and the whole infrastructure is protected with 2FA and SSO.

29. How do you ensure all flows of personal and special category data are documented including where data was obtained and all destinations of data?

This is stored in our GDPR compliant data inventory.

30. Is all sensitive information identified (e.g. by protective marking) and properly protected?

Intelliflo owned personal data is only stored within Intelliflo contracted SaaS systems, such as Salesforce and Netsuite. Your clients personal data is stored within the iO platform. We have business rules specifying what data is stored where.

31. Describe how your processes allow data subjects to request changes to incorrect data or deletion of data?

This is outlined in our privacy notices, data subjects contact dataprotection@intelliflo.com - this is the same address to exercise all data subject rights. We follow the ICO guidance on identifying the data subject, once we have done this we triage the request, and treat it appropriately for the type of request. We track data subject rights requests as tickets within our support ticketing system, and we report on SLAS in our board report.

32. When assets are no longer required, is all data securely wiped from them or are the assets securely destroyed?

(Special software can be used to securely wipe data and external companies can be used to provide a secure destruction service.)

Yes, this is covered by our asset management policy - which specifies destruction of all devices which could contain data at end of life.

Cloud services

33. Do you use a public cloud provider to store or share files and information between employees?

Yes, Intelliflo uses some cloud providers or products, including Microsoft Office 365, Salesforce, JIRA, Slack and Jitterbit that communicate some incidental PII data where Intelliflo is acting as the data processor on behalf of our customers, typically to investigate issues.

Intelliflo also uses Microsoft Office 365, Salesforce, JIRA, Netsuite and Jitterbit where Intelliflo is the data processor, e.g. data about our customers. When Intelliflo is securely exchanging large volumes of data with clients then Maytech Quatrix is used and the data is securely stored for 2 weeks by the provider before being deleted.

If you are not happy with incidental client data being stored in Microsoft Office 365, or Salesforce - you should not send it to us in support tickets or via email.

34. Where is the data that is sent to a public cloud provider stored?

We only use EEA instances or regions of public cloud providers for data storage, for example, we use AWS eu-west, Salesforce EU13 or Netsuite EU2.

If you use your own AWS storage buckets, it is your responsibility to make sure these are in the EEA and that your bucket is configured securely. Where we do use cloud providers in the US, we make sure they are certified EU-US privacy shield providers.

35. If you store personal data with your cloud provider, do you store any of that data outside of the European Economic Area (EEA)?

As our answer to 34 above, Intelliflo does not mandate the systematic storage of customer data with cloud providers outside the EEA.

If a firm's customers use the PFP premium capability through the Yodlee integration then client data would be delivered from the U.S. Yodlee is an EU-US Privacy Shield certified member meaning such data storage is compliant with the GDPR.

<https://www.privacyshield.gov/participant?id=a2zt0000004E3SAAU&status=Active>

36. If yes to the above, have you obtained explicit consent from data subjects to transfer their data outside of the European Economic Area (EEA)?

Using only consent to protect data transfer outside the EEA is regarded as a weak protection of the rights of data subjects. Consent is required by GDPR Article 49 as a last resort, if better protections such as adequacy decisions, model clauses or other legal protection cannot be put in place.

This is because a data subject has to consent, unless better protections cannot be put in place. We would only store data outside the EEA if we had adequate protection in place - for example via model clauses, adequacy decisions or privacy shield.

For more details on this - please read GDPR articles 44 to 49 covering international transfers.

37. If yes to the above, does your provider certify to an agreement such as EU-US Privacy Shield or to other binding corporate rules that confirm the level of protection given to that data?

As above, Yodlee are a certified Privacy Shield EU-US firm.

<https://www.privacyshield.gov/participant?id=a2zt00000004E3SAAU&status=Active>

38. Do the public cloud providers that your organisation uses hold any recognised security accreditations?

- Microsoft - numerous
<https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001>
- Salesforce - numerous
<https://trust.salesforce.com/en/compliance/>
- Netsuite - numerous
<http://www.netsuite.co.uk/portal/uk/platform/infrastructure/operational-security.shtml>
- Amazon Web Services - numerous
<https://aws.amazon.com/compliance/pki-data-privacy-protection-hipaa-soc-fed-ramp-faqs/>

Generally ISO 27001 is our minimum baseline.

39. Is your data encrypted before being passed between your site and the public cloud provider (i.e. encrypted in transit)?

Yes, all Intelliflo services will use TLS v1.2 to communicate with downstream services where the downstream services support this.

40. Is your data encrypted whilst being stored or processed by the public cloud provider (i.e. encrypted at rest)?

Where Intelliflo is processing data on behalf of our customers then data is always encrypted where it is stored in the cloud by Intelliflo either systematically or incidentally.

Where Intelliflo is the data controller, specifically data about our customers, encryption is employed by our cloud providers - such as Microsoft, Salesforce, Netsuite, Slack.

Risk management

41. Do you have a current risk assessment?

Yes, Intelliflo operate a risk register. This is updated and progressed at least monthly with new high priority risks reported to the board monthly.

This process is certified to ISO 27001 as part of Intelliflo's ISO 27001 ISMS.

42. Has your risk assessment been reviewed in the last 12 months?


Yes, this is monthly, and reported upon in the COO's board pack.

43. Does the risk assessment cover the scope of this assessment?

Yes, the risk assessment covers the full scope of the business.

44. Was the risk assessment approved at Board Level?

Yes, risk progress is reported to the main board monthly, the CEO reviews the highest priority risks annually.



Protection

45. Have you put policies and procedures in place to mitigate risks to personal data?

Yes, we have multiple policies and procedures to mitigate risks to personal data. These include sending data via a file sharing portal.

46. Are these policies and procedures provided to all employees to be followed in everyday practice and linked to disciplinary procedures?

Yes. There are policies and procedures provided to employees via Confluence which allow them to view the employee handbook which details these.

47. Is data protection referred to in employee contracts of employment?

Employee contracts state that policies and procedures in the company handbook will be adhered to, which includes data protection.

48. Do policies and procedures set clear responsibilities for handling of personal data, including where appropriate reference to responsibilities held by your Data Protection Officer?

Yes. We have clear roles and responsibilities for data protection and information security, these are managed as part of our ISO 27001 certified Information Security Management System.


49. When your organisation collects personal data from a subject do you clearly state what it is being collected for, how it will be processed and who will process it and does the data subject have to provide consent for this?

Yes, this is covered in our privacy policies. These are currently being updated for GDPR compliance.

It is important to note that we are your (our clients) data processor - hence we do not have privacy policies which cover your operations. Our grounds for processing your data are following the legal instruction of a data controller.

50. Where you collect data from children (subjects under 16 in the UK) do you actively seek parental consent?

Intelliflo as a data controller does not collect or hold data related to people who are under 16.



51. Does your risk assessment cover the management of personal data or special category data?

Yes, we ensure our risk assessment (PIA) process covers the management of personal and special category data.

52. Do you have a process for dealing with Subject Access or Data Portability Requests within an appropriate timescale? Under data protection legislation, individuals have a right to obtain a copy of the information you hold about them

Yes, this will be covered in our privacy policies.

You will need a process for serving subject access requests for the data you hold within iO.

53. Do you have a process for correcting inaccurate records, deleting records or suspending the processing of records? Under data protection legislation, individuals have the right to have inaccuracies corrected and may have the right to have information about them deleted from systems

Yes, this will be covered in our privacy policies - this only applies to data for which we are the data controller.

You will need a process for correcting the data you hold within iO.

54. Do you have documented data retention periods, do these cover contractual and legal requirements?

Yes, this is covered in our privacy policies.

55. Do you have documented data classification criteria?

Yes, customer data is one of the categories subject to the strongest security controls.

56. Do you have a data protection or data privacy statement compliant with the requirements of the GDPR and does the statement provide a point of contact for data protection issues?

Yes, our data protection policy has been updated to be GDPR compliant and we have provided contact details for the Intelliflo DPO.



57. Where you are holding data based upon the consent of the data subject, how do you record details of the consent?

Consent is stored in the various systems which we use to manage the data.

We do not use consent as a basis to handle your data - we are a processor for your data, so do not need a legal basis to hold this data. Intelliflo is following the lawful instruction of a data controller (you, our client).

58. Do you have mechanisms in place which make it as easy for the data subject to remove consent for data processing and do you ensure it is as easy to remove consent as it was for them to give it?

We have an unsubscribe button at the bottom of emails to ensure it is as easy to remove consent as it is to give it.

59. For each piece of personal information you hold, do you record the purpose for which it was obtained?

Our data is mainly held for legitimate interests. If it is not we would record the purpose.

60. For each piece of personal information you hold, do you record the justification for obtaining it?

Justifications for obtaining the information might include explicit consent, contract fulfilment, performing a public function, meeting a legal requirement or another legitimate interest.

Yes, we hold a data inventory which would include this.

61. For each piece of special category data you hold, do you record the justification for obtaining it?

Justifications for obtaining special category (or sensitive personal data) could include specific consent, use for employment purposes or to meet a medical need.

Yes, this is covered in our data inventory.

62. For each piece of personal information you hold, do you record whether your organisation is the data processor or the data controller?

Yes, this is covered in our data inventory.



63. In each contract you hold with suppliers and customers involving the processing of personal data, do you confirm whether you are the data controller or data processor?

In our standard client contract, we specify that we are the data processor.

In our standard supplier contract, we specify that we are the data processor and they are our sub-processor.

64. Where you disclose personal data to a supplier/provider does the contract explicitly impose the obligation to maintain appropriate technical and organisational measures to protect personal data in line with relevant legislation?

This is in our standard supplier contract, in line with our GDPR requirements as your sub processor to manage our processors.

People

65. Do you take up references and/or confirm employment history when employing new staff?

Yes. We ensure that we have two references from any new employees and look at their employment history.

66. Where criminal record checks are carried out, do you ensure that explicit consent has been obtained from employees and that such checks are carried out for lawful purposes?

We use a service called Verifile, a 3rd party agency, to screen all prospective employees. This includes:

- Employer reference checks, employer's name and address, period of employment
- Position held
- Reason for leaving
- Disciplinary action taken against the candidate
- Re-employment of the candidate by the employer
- Absence, salary and a number of other questions
- Criminal record check
- Basic disclosure: searches of the Police National Computer which discloses all convictions that are not spent under the Rehabilitation of Offenders Act. It discloses all such convictions, or states that there are none
- Standard identity and financial check. The Electoral Roll to verify a candidate's current and previous addresses
- Publicly available data covering the last 6 years to reveal adverse information, including County Court Judgments, bankruptcies and voluntary arrangements.
- Checks for adverse records at addresses that are linked to the candidate and may have not been disclosed by the candidate.
- Any aliases linked to the candidate.

In a scenario where a prospective employee did not pass, we would initially talk to them about the issues which may have been found. However, all offers are conditional to a user passing their screening, so if we were not happy they would not be hired and we have historically rejected candidates on the basis of their Verifile screening.

67. Is there someone responsible for security training/awareness?

HR take responsibility for this. This is audited as part of our ISO 27001 ISMS.

68. Is security training refreshed regularly? Describe how this is done

Yes, this is managed via Intelliflo eLearning academy. The LMS hosts the courses which have a 1 year validity after which employees are asked to do them again. This is done annually, monitoring by the Intelliflo HR department and audited as part of our ISMS.

All Intelliflo staff are trained in data protection, information security, anti bribery and phishing awareness.

69. Do you give new employees a briefing on their corporate and security responsibilities before, or immediately after employment, preferably reinforced by reference literature?

Yes. This happens in the induction process.

70. Do employee contracts include security obligations (such as an obligation to comply with the security policy) and are reminders given at regular intervals?

Yes, all security obligations are laid out in the employee handbook which all employees are required to read. When policies are updated or changed, employees are sent notifications to read and agree the changes. All employees are required to complete security training annually.

71. Are employees with special responsibility for security, or with privileged access to business systems adequately trained/qualified?

Yes, Intelliflo have an in depth training plan. All staff are trained in information security.

72. On termination of employment, are user access privileges immediately withdrawn and the employee de-briefed on their post employment confidentiality responsibilities?

Yes. As soon as employment is terminated all user access privileges are withdrawn and there will be a leaving meeting with the employees manager. User access privileges will be taken away at the end of the working day on the employees last day of employment.

Security policy

73. Do you have a current security policy? A security policy can be stand-alone or incorporated into other policy, but it should set out your objectives for managing your security.

Intelliflo has a number of security related policies which make up Intelliflo's Information Security Management System (ISMS). The Intelliflo ISMS has been certified by BSI as compliant with ISO 27001.

74. Has your policy been reviewed in the last 12 months?

Yes, our policies are reviewed annually and this is audited as part of our ISMS.

75. Does the policy cover the scope of this assessment?

Yes, the scope of the ISMS is the whole business.

76. Was the policy approved at board level? Provide the name and role of the person who approved this policy.

Yes, our COO, Robert Walton approves our policies as owner of the ISMS.

77. Is there a policy review and consultation process?

Yes. The policies are reviewed and then approved by our COO.

78. Does the policy refer to Intellectual Property Rights and legal requirements?

This is included in our policy for working in secure areas.

79. Does the policy refer to personnel security?

Yes, the security policies cover personnel security and are audited as part of our ISO 27001 ISMS.

80. Does the policy refer to asset management?

Yes, the policies cover asset management and are audited as part of our ISO 27001 ISMS.



81. Does the policy refer to access management?

Yes, the policies cover access management and are audited as part of our ISO 27001 ISMS.

82. Does the policy refer to physical and environmental security?

Yes, the policies cover physical security and are audited as part of our ISO 27001 ISMS.

83. Does the policy refer to computer and network security?

Yes, the policies computer and network security and are audited as part of our ISO 27001 ISMS.

84. Does the policy refer to security from malware and intrusion?

Yes, the policies cover malware and intrusion and are audited as part of our ISO 27001 ISMS.

85. Does the policy refer to security incident management?

Yes, we have an incident management policy which covers all types of incident including security. This is audited as part of our ISO 27001 ISMS.

86. Does the policy refer to business continuity measures?

Yes, we have a tested BCP plan. This is audited as part of our ISO 27001 ISMS.

87. Does the policy refer to handling personal data (and, where appropriate, reference your data protection policy)?

Yes, our company handbook covers how people should handle personal data. This includes specific rules of engagement for how to behave when handling customer data held within the Intelligent Office platform. This is audited as part of our ISO 27001 ISMS.

88. Is the policy distributed to all employees?

The policy is on Confluence for all employees to see.

89. Is the security policy part of all employees' contractual obligations?

Yes, this is covered in our standard employment contract. Additionally it extends beyond their period of employment.



90. Do the contracts with all your suppliers ensure that they meet the requirements of your security policy around handling data and keeping information secure?

Yes, security is a part of all partners and suppliers contractual obligations.

91. Are there business sector-specific laws/regulations relating to risk treatment or information security which apply to your business?

We are covered by the General Data Protection Regulation, and the National Infrastructure Services directive. Both of these require us to manage data protection and information security risks.

92. Are there UK or EU laws/regulations relating to risk treatment or information security which apply to your business?

We are covered by the General Data Protection Regulation, and the National Infrastructure Services directive. Both of these require us to manage data protection and information security risks.

93. Are there other international legislation/regulations relating to risk treatment or information security which apply to your business?

Yes, the National Infrastructure Services Directive applies to Intelliflo who are a Digital Service Provider.

94. Do you store credit card information?

No, we do not store credit cards, and are not regulated by PCI-DSS.

95. If yes to above, are the systems that you use to store credit card information compliant to PCI-DSS regulation?

We do not store credit cards, and are not regulated by PCI-DSS.

96. Is your business part of a public global organisation that is required to have external financial reporting?

No.



Physical and environmental protection

97. Are only authorised personnel who have a justified and approved business case given access to restricted areas containing information systems or stored data?

Yes, access to locations containing sensitive data is restricted.

Customer data is only kept in Intelliflo's data centres, an extremely limited number of people have physical access to these sites.

98. Are devices which require particular working conditions - such as heating and cooling - provided with a suitable environment within the guidelines set out by their respective manufacturers?

Yes, this is part of Intelliflo's ISO 27001 ISMS.

99. Do all business premises have effective physical protection and, if indicated by a risk assessment, surveillance and monitoring?

Yes, this is audited as part of Intelliflo's ISO 27001 ISMS.



Office firewalls and internet gateways

- 100. Do you have firewalls at the boundary between your organisations internal networks and the internet? You should have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network. Remember most internet-routers contain a firewall.**

Yes, we have firewalls in place on our security boundaries. Remote workers can only access certain systems via the VPN, other systems can be directly connected to over the internet via a secure and encrypted SSL connection and only where two-factor authentication (2FA) is in place.

- 101. When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices?**

Yes, this is in place.

- 102. Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess? A password that is difficult to guess will not be made up of common or predictable words such as “password” or “admin”, or include predictable number sequences such as “12345”**

Yes, our best practice for service accounts like this, is to use very long randomly selected passwords which are at least 32 characters long and with entropy of at least 100 bits. These are then stored in a password safe.

- 103. Do you change the password when you believe it may have been compromised?**

Yes.

- 104. Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case?**

At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a server or a video conferencing unit). This is sometimes referred to as “opening a port”. You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer “No”. If yes to above, do you have a process to ensure they are disabled in a timely manner when they are no longer required?

No, only services which are required to be public to the internet are public to the internet. Only a very limited number of external services are exposed for internal purposes. Furthermore, we have daily scanning of the Intelliflo internet facing profile, by a 3rd party security firm, and any changes are flagged to the Intelliflo security team and must be confirmed as being known and expected. All externally visible systems are also subject to 3rd party vulnerability and penetration tests.

105. If yes to above, do you have a process to ensure they are disabled in a timely manner when they are no longer required?

Yes, they are removed as services are decommissioned.

106. Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet? By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.

Yes, we only permit a limited range of services to be visible to the internet. Furthermore, we have daily scanning of the Intelliflo internet facing profile, by a 3rd party security firm, and any changes are flagged to the Intelliflo security team and must be confirmed as being known and expected.

**107. Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?
Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer “no” to this question.**

Yes, we use outsourced firewall support from two partners. This gives us strong segregation of duties between Intelliflo employees and the people who operate our firewall rules.

108. If yes, is there a documented business requirement for this access?

This access is to permit the suppliers who run these devices to access these devices

109. If yes, is the access to the settings protected by either two-factor authentication or by only allowing trusted IP addresses to access the settings?

Yes, IP restrictions are in place.

Software firewalls

110. Do you have software firewalls enabled on all of your computers and laptops?

You can check this setting on Mac laptops in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings or Control Panel and searching for “windows firewall”.

Yes, these are part of the standard build. Users cannot turn these off.

111. If no, is this because software firewalls are not commonly available for the operating system you are using?

We use the Windows or Linux firewalls whichever is applicable.



Secure configuration

- 112. Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? This includes applications, system utilities and network services.**

Yes, we have a standard build. This is the operating system plus a number of applications required for users to do their jobs.

- 113. Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business?**

Yes, this is part of the standard build. User devices are hardened to the Microsoft Security Compliance Manager baseline.

- 114. Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?**

Yes, we use Microsoft LAPS to manage administrators passwords and ensure they are all different.

- 110. Do all your users and administrators use passwords of at least 8 characters? A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.**


Yes, we require users to use passwords with 12 or more characters (corporate), or 14 or more characters (hosting networks). We use standard complexity requirements - 3 of upper/lower/special/numeric, and use a password filter to block common passwords.

- 111. Do you run software that provides sensitive or critical information (that shouldn't be made public) to internet based users?**

Yes, we use a tool called Maytech Quatrix for distribution, and receipt, of client data to/from Intelliflo customers.

- 112. If yes, do you ensure all users of these services use a password of at least 8 characters and that your systems do not restrict the length of the password?**

Yes, we require all staff accounts to be 12 or 14 characters in length, additionally we use mandatory 2FA.



113. If yes, you ensure that you change passwords if you believe that they have been compromised?

Yes.

114. If yes, are your systems set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?

Yes, we lock out after 10 failed attempts and the account is blocked for 30 minutes. In addition we require multi-factor authentication (MFA) for logins to workstations or laptops, remote access, and all corporate cloud services.

115. If yes, do you have a password policy that guides all your users?

The password policy must include: guidance on how to choose non-guessable passwords, not to use the same password for multiple accounts, which passwords may be written down and where they can be stored, and if they may use a password manager.

Yes, this is part of our staff handbook which staff are required to read.

116. Is “auto-run” or “auto-play” disabled on all of your systems?

This is a setting which automatically runs software on a DVD or memory stick. You can disable “auto-run” or “auto-play” through control panel / system preferences.

Yes, this is disabled per our standard build.



Patches and updates

122. Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?

Yes.

123. Are all applications on your devices supported by a supplier that produces regular fixes for any security problems?

Yes, we use a tool called Ninite Pro to manage updates for a huge number of non-Microsoft applications. This is installed on all user devices running Windows, which ensures that users are always running up to date versions of applications. This covers the core malware vectors of Flash, Adobe Reader and Java. Flash and Java auto run is also disabled, to give further defence in depth here.

124. Is all software licensed in accordance with the publisher's recommendations?

Yes, additionally around 80% of users have no ability to install software as they have no admin privileges.

125. Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release?

Yes.

126. Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release?

Yes, these are either done via our OS patching processes or handled by Ninite Pro.

127. Have you removed from all of your devices any applications that are no longer supported and no longer receive regular fixes for security problems?

Yes.



Operations and management

128. Is management of computers and networks controlled using documented procedures that have been authorised?

Yes, this is audited as part of our ISO 27001 certified ISMS.

129. Does the organisation ensure that all new and modified information systems, applications and networks include security provisions, are correctly sized, comply with security requirements, are compatible with existing systems and are approved before they commence operation?

Yes, this is an ISO 27001 requirement. This is handled through our capacity management, change control and secure development processes.

130. Where personal data is in use, do you ensure that a Privacy Impact Assessment is carried out for new systems and projects?

Either where we are the data controller or where we would be the data processor for the personal data privacy, assessments are completed for system implementations or significant changes to existing systems.


131. Are changes to information systems, applications or networks reviewed and approved?

Yes, this is handled via our change control process.

132. Where data storage, applications or other services are provided by another business (such as a cloud provider), is there independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those used by your organisation?

An example of such confirmation is an independent audit of the whole business to ISO27001 or the IASME audited standard.

Yes, we require ISO 27001 for suppliers who hold or process our data or evidence of an equivalent level of security management.



User accounts

133. Are users only provided with user accounts after a process has been followed to approve their creation?

Yes, this is part of the new starters process whereby only HR can create initial account creation requests.

134. Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?

Yes, users have unique accounts, additionally they use MFA to login alongside their regular account.

135. Have you deleted, or disabled, any accounts for staff who are no longer with your organisation? When an individual leaves your organisation you need to stop them accessing any of your systems.

Yes, this is part of our leavers process. Accounts are disabled at the end of a leavers last day.

136. Do you ensure that staff only have the privileges that they need to do their current job? When a staff member changes job role you may also need to change their access privileges.

Yes, we have a rights approval process.



Administrative accounts

137. Do you have a formal process for giving someone access to systems at an “administrator” level?

Yes, very limited numbers of people have this access and this access is by role.

138. Do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?

Yes, administrator accounts are not used for day to day usage and there is both monitoring and alerting in place to identify when the accounts are accessed.

We generate alerts when domain administrator accounts are used on none domain controller devices, or when new domain administrator accounts are created.

139. Do you ensure that administrator accounts are not used for accessing email or web browsing?

Yes, administrators have separate accounts for internet access and privileged access.

We generate alerts when domain administrator accounts are used on none domain controller devices, or when new domain administrator accounts are created.

140. Do you formally track which users have administrator accounts in your organisation?

Yes, a very limited list of staff have administrator access.

141. Do you review who should have administrative access on a regular basis?

Yes, we review this annually as part of our penetration test.

142. Have you enabled two-factor authentication for access to all administrative accounts?

Yes, all user accounts including standard user accounts as well as administrator accounts require 2FA. We use Duo Security Multi Factor Authentication. Additionally we have disabled SMS and phone as a factor in line with NIST recommendations.

143. If no, is this because two-factor authentication is not available for some or all of your devices or systems?

As per 142 above, we use 2FA.



- 144. Are all of your computers, laptops, tablets and mobile phones protected from malware by either A - having anti-malware software installed, B - limiting installation of applications to an approved set (ie using an App Store or application whitelisting) or C - application sandboxing (ie by using a virtual machine)? Its usually easiest to protect computers and laptops from malware by using A. Tablets and mobile.**

Yes we use anti-malware software everywhere, we use Windows Defender on desktops and Symantec Endpoint Protection in our hosting environment.

No customer data is stored on user machines or on the same networks as the user devices.

- 145. (A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access? This is usually the default setting for anti-malware software.**

Yes, windows defender and Symantec are set to take updates as they arrive.

- 146. (A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?**

Internet Explorer is protected by Microsoft SmartScreen, and Chrome users have similar protection native to Chrome.

We additionally implement Quad9 DNS blocking, and Alertlogic IDS. No customer data is stored on user machines or on the same networks as the user devices.

- 147. (B) Where you use an app-store or application signing, are users restricted from installing unsigned applications? By default, most mobile phones and tablets do not allow you to install unsigned applications. Usually you have to “root” or “jailbreak” a device to allow unsigned applications**

We block the windows app store, 80% of our users are not local administrators and cannot install any applications.

All mobile devices are blocked from being jailbroken. No customer data is stored on the machines and networks on which users can install applications.

148. (B) Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?


We don't permit users to access the Windows store, 80% of our users are not local administrators and cannot install any applications.

No customer data is stored on the machines and networks on which users can install applications.

149. (C) Where you use application sandboxing, do you ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and your local network? If you are using a virtual machine to sandbox applications, you can usually set these settings within the configuration options of the virtual machine software.

We don't use application sandboxing.

No customer data is stored on the machines and networks on which users can install applications.



Vulnerability scanning

150. When was the last time you had a vulnerability scan on your system?

We have monthly vulnerability scans, these are provided by NCC Group. We have annual penetration tests, the last one of these was in December 2017. Every year we use a 3rd party to run red team breach tests. The last one was in March 2017.

To understand the difference between a penetration test and a red team test please go [here](#).

151. Did you act to improve the security of your system on the basis of the scan results?

Yes, this feeds into our vulnerability and risk management process.



Monitoring

152. Does the organisation regularly review event logs?

Yes, security logs are sent to AlertLogic who run a 24x7 security operations centre. AlertLogic escalate critical issues back to us.

153. Is an audit trail of system access and/or data use by staff maintained and reviewed on a regular basis?

Yes, log data across systems and technology layers is stored in the Intelliflo Splunk instances and also sent offsite, in duplicate, to AlertLogic who run a 24x7 security operations centre. The usage and access data is reviewed in real time and any anomalies are alerted to Intelliflo.

Backup and restore

154. Are data stored on the business premises backed up regularly (at least weekly) and restores tested at appropriate intervals (at least monthly)?

Yes, we backup all critical data sets and we perform weekly restores of our customer databases as part of our routine database maintainance processes.

155. Are all backups secured with an appropriate level of protection for the type of data they contain?

Yes, all backups are only stored on backup devices, and encrypted with AES256 GCM when they are stored offsite.

156. Is a backup copy held in a different physical location?

Yes, we hold critical backups at both of our sites, and backups are stored offsite to AWS S3.



Incident management

157. Are users who install software or other active code on the organisation's systems without permission subject to disciplinary action?

Yes, this is covered in our company handbook. Most (more than 80%) users do not have the permissions, so cannot do this.

158. Are all breaches of the security policy and other information security incidents or suspected weaknesses reported and recorded?

Yes, this is handled through our incident management process. We categorise incidents by root cause and use this data to drive process improvements.

159. What is your process for reporting losses of personal data to the Information Commissioner (or your national data protection authority) and the data subjects?

Once we have determined that a data breach has occurred, how many and what types of records and what system we would do the following:

In the case that the breach affected client data (the data for which we are a processor) we would inform our clients via our account managers, who would then inform the Information Commissioner.

In the case that the breach affected our data (the data for which we are a controller), we would engage our DPO and contact the ICO using the latest process specified on the website of the Information Commissioner.

160. Are information security incidents investigated to establish their cause and impacts with a view to avoiding similar events?

Yes, this is handled through our incident management process, and includes near misses as these are opportunities for improvement and valuable datapoints.

161. If required as a result of an incident, is data isolated to facilitate forensic examination?

Intelliflo have contracted with a third party security incident response specialist, MWR Inforsecurity, who would provide expert guidance in the event of an issue. This is contracted on a 24/365 4hr response model. As a result of the Intelliflo architecture it is possible to easily recover the platform while isolating infrastructure for forensic analysis.

162. Is a record kept of the outcome of all security incident investigations?

Yes, this is handled through our incident management process. All security events or service impacting issues cause an incident timeline to be written, which permits us to track and identify root causes and trends.

Business continuity

163. Does the organisation ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks?

Yes, we operate an active deployment model for our SaaS platform . This means we run at all times from two sites, so that the loss of any single site does not impact customer operations.

164. Does the organisation review the business continuity and disaster recovery plans at least once per year?

Yes, this is audited as part of our ISO 27001 ISMS.

165. Does the organisation exercise the business continuity and disaster recovery plans at least once per year?

Yes, for example we last did a full site failover test in August 2017, this is audited as part of our ISO 27001 ISMS.

