



GDPR Assessment

Risk Treatment Plan



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the organisation specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the organisation or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company







1/18/2018















Risk Treatment Plan

The Risk Treatment Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

Risk Score	Recommendation	Severity	Probability
100	GDPR Regulation (EU) 2016/679 Article 5 - Principles relating to processing of personal data Ensure that personal data is processed in a manner that complies with these principles related to data processing. <ul style="list-style-type: none"> <input type="checkbox"/> Lawfulness, Fairness, and Transparency <input type="checkbox"/> Purpose Limitation 	H	H
100	ISO 27001-2013 (9.2.5) - Inventory of assets Investigate and remove all users that are not authorised. <ul style="list-style-type: none"> <input type="checkbox"/> phugo : Pepe Hugo <input type="checkbox"/> hmorris : Horace Morris 	H	H
95	ISO 27001-2013 (8.3.1) - Management of removable media ISO 27001-2013 (8.3.2) - Disposal of media ISO 27001-2013 (11) - Physical and environmental security Address the issues found during the walk-through of the physical environment. <ul style="list-style-type: none"> <input type="checkbox"/> Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1) <input type="checkbox"/> Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2) <input type="checkbox"/> Servers or devices containing sensitive information reside in an insecure area (11.1.1a) <input type="checkbox"/> Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b) <input type="checkbox"/> Lack of physical access control either manned or unmanned (11.1.1c) <input type="checkbox"/> Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e) <input type="checkbox"/> Lack of physical intrusion detection system (11.1.1f) <input type="checkbox"/> Processing facilities maintained by external parties co-located with the organizations information processing facilities (11.1.1g) <input type="checkbox"/> Visitors allowed entry to secured areas without recording date and time (11.1.2a) 	H	H

Risk Score	Recommendation	Severity	Probability
	<ul style="list-style-type: none"> <input type="checkbox"/> Visitors allowed to move unsupervised through secured areas (11.1.2a) <input type="checkbox"/> Lack of authentication mechanism to secure areas (11.1.2b) <input type="checkbox"/> Lack of physical or electronic audit trail for all access to secure areas (11.1.2c) <input type="checkbox"/> Employees, contractors, or external parties in secure area without visible identification (11.1.2d) <input type="checkbox"/> Un-monitored third parties in secure areas (11.1.2e) <input type="checkbox"/> Direct access by public to key facilities (11.1.3a) <input type="checkbox"/> Obvious signage indicating the presence of information processing activities (11.1.3b) <input type="checkbox"/> Computer monitors positioned such that they are visible from outside the facility (11.1.3c) <input type="checkbox"/> Directories or internal telephone books identify locations of confidential information processing facilities readily accessible to unauthorised personnel (11.1.3d) <input type="checkbox"/> Computer monitors are positioned such they are visible from unauthorised persons during their use (11.2.1b) <input type="checkbox"/> Storage facilities are not secured to prevent unauthorised access (11.2.1c) <input type="checkbox"/> Lack of cabling security could allow unauthorised access (11.2.3) <input type="checkbox"/> Sensitive information on paper found in unlocked areas (11.2.9a) 		
92	<p>ISO 27001-2013 (12.2.1) - Controls against malware Enable anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of GDPR Compliance report.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DESKTOP-T4V0EQD / fe80::fd6c:e966:5fd8:41dd%17,fe80::7129:45d7:faf3:8fe6%16,169.254.65.221,10.0.5.156 / Windows 10 Pro <input type="checkbox"/> ACCT-2017 / fe80::31ad:c0f1:83f5:abf8%12,10.0.1.18 / Windows Server 2012 R2 Datacenter 		
92	<p>ISO 27001-2013 (12.2.1) - Controls against malware Ensure anti-virus programs on the computers indicated in the Endpoint Security section of the Evidence of GDPR Compliance report are up-to-date.</p> <ul style="list-style-type: none"> <input type="checkbox"/> ACCT-2017 / fe80::31ad:c0f1:83f5:abf8%12,10.0.1.18 / Windows Server 2012 R2 Datacenter 		
90	<p>ISO 27001-2013 (12.2.1) - Controls against malware Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorised access and the spread of malicious software. Many is defined as missing three or more patches.</p>		

Risk Score	Recommendation	Severity	Probability
90	GDPR Regulation (EU) 2016/679 Article 7 - Conditions for consent Ensure that the processing of personal data has explicit consent.		
89	ISO 27001-2013 (12.4.3) - Administrator and operator log Enable auditing of all actions taken by any individual with root or administrative privileges.		
87	ISO 27001-2013 (13.1.1) - Network controls Block web traffic to all sites not required by the DPE. <ul style="list-style-type: none"> <input type="checkbox"/> http://download.cnet.com <input type="checkbox"/> http://gmail.google.com <input type="checkbox"/> http://mail.yahoo.com <input type="checkbox"/> http://www.facebook.com <input type="checkbox"/> http://www.myspace.com <input type="checkbox"/> http://www.playboy.com <input type="checkbox"/> http://www.tucows.com <input type="checkbox"/> http://www.youporn.com <input type="checkbox"/> http://www.youtube.com <input type="checkbox"/> https://plus.google.com 		
85	ISO 27001-2013 (9.4.5) - Access control to program source code Adhere to the best practises regarding access control to program source code. <ul style="list-style-type: none"> <input type="checkbox"/> Program source libraries are not held in operational systems <input type="checkbox"/> Support personnel do not have unrestricted access to program source libraries <input type="checkbox"/> An audit log is maintained of all accesses to program source libraries <input type="checkbox"/> Maintaining and copying of program source libraries should be subject to strict change control procedures 		
85	ISO 27001-2013 (7.2.2) - Information security awareness training Provide security awareness and training for employees and contractors, if relevant, and provide appropriate records and documentation.		
85	ISO 27001-2013 (5.1.2) - Review of the policies for information security Maintain documentation of when and which authorities to contact and how identified information security incidents should be reported in a timely manner.		
83	ISO 27001-2013 (16) - Information security incident management Document information security incident management		

Risk Score	Recommendation	Severity	Probability
	procedures. See ISO 27001-2013 (16) for additional guidance.		
80	ISO 27001-2013 (6.1.5) - Information security in project management Integrate information security into the project management methodology to ensure risks are identified and addressed.	H	H
80	GDPR Regulation (EU) 2016/679 Article 13 - Information to be provided where personal data are collected from the data subject Article 14 - Information to be provided where personal data have not been obtained from the data subject Ensure that the Privacy Policies has the required elements. <ul style="list-style-type: none"> <input type="checkbox"/> DPO Contact Details - the contact details of the data protection officer, where applicable. <input type="checkbox"/> Legitimate Interest - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party. <input type="checkbox"/> Intent to Transfer (if applicable) - where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. <input type="checkbox"/> Obligation and Consequences to Data Subject - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data. <input type="checkbox"/> Existence of Automated Decision-Making - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. <input type="checkbox"/> Indirectly Obtained Personal Data Notice - notice that personal data obtained not directly from the obtained from the data subject also confirms to the above provisions. 	H	H
80	ISO 27001-2013 (10.1) - Cryptographic controls Document cryptographic control procedures, including key management.	H	H
77	ISO 27001-2013 (9.4.3) - Password management system Ensure password lockout is enforced after more than six attempts. <ul style="list-style-type: none"> <input type="checkbox"/> DC13 	M	H

Risk Score	Recommendation	Severity	Probability
	<input type="checkbox"/> DCMC01 <input type="checkbox"/> DESKTOP-N6S4H9A <input type="checkbox"/> DESKTOP-T4V0EQD <input type="checkbox"/> ENGWORKS <input type="checkbox"/> HP-DT201702-01 <input type="checkbox"/> INFIT1 <input type="checkbox"/> JASONB-PC <input type="checkbox"/> ORBIT <input type="checkbox"/> MYCOSPARE001 <input type="checkbox"/> MYCOWDS12 <input type="checkbox"/> PSOLSTICE-PC <input type="checkbox"/> ACCT-2017 <input type="checkbox"/> MCGATEWAY <input type="checkbox"/> MCVDS <input type="checkbox"/> MCVDS2 <input type="checkbox"/> ROBIT <input type="checkbox"/> STORAGE15 <input type="checkbox"/> VPNGW <input type="checkbox"/> WILLEP		
75	ISO 27001-2013 (17.1) - Information security continuity Document information security incident management procedures. See ISO 27001-2013 (16) for additional guidance.	H	H
75	ISO 27001-2013 (8.3.3) - Physical media transfer Adhere to the following best practises for physical media transfer. <ul style="list-style-type: none"> <input type="checkbox"/> Physical media transfer (ISO 27001-2013 A.8.3.3) 	H	H
74	ISO 27001-2013 (9.4.3) - Password management system Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. <ul style="list-style-type: none"> <input type="checkbox"/> BBRONSOND-PC <input type="checkbox"/> SKYHIGH-PC <input type="checkbox"/> DC13 <input type="checkbox"/> DCMC01 <input type="checkbox"/> DESKTOP-N6S4H9A <input type="checkbox"/> DESKTOP-T4V0EQD <input type="checkbox"/> ENGWORKS <input type="checkbox"/> HP-DT201702-01 <input type="checkbox"/> INFIT1 <input type="checkbox"/> JASONB-PC <input type="checkbox"/> ORBIT <input type="checkbox"/> MYCOSPARE001 <input type="checkbox"/> MYCOWDS12 <input type="checkbox"/> PSOLSTICE-PC <input type="checkbox"/> ACCT-2017 <input type="checkbox"/> MCGATEWAY <input type="checkbox"/> MCVDS 	M	H

Risk Score	Recommendation	Severity	Probability
	<input type="checkbox"/> MCVDS2 <input type="checkbox"/> ROBIT <input type="checkbox"/> STORAGE15 <input type="checkbox"/> VPNGW <input type="checkbox"/> WILLEP		

Medium Risk

Risk Score	Recommendation	Severity	Probability
70	ISO 27001 – 11.2.8 Unattended user equipment Enable automatic screen lock on the specified computers. <ul style="list-style-type: none"> <input type="checkbox"/> DC13 <input type="checkbox"/> DCMC01 	H	M
70	ISO 27001-2013 (9.4.1) - Information access restrictions Investigate and either disable or note compensating controls to ensure these potential generic accounts are not used inappropriately. Service accounts are excluded. <ul style="list-style-type: none"> <input type="checkbox"/> .administrator <input type="checkbox"/> .admin 	M	M
70	GDPR Regulation (EU) 2016/679 Article 7 - Conditions for consent Enter a documented reason for the processing of personal data in the GDPR Compliance Questionnaire.	M	M
69	ISO 27001-2013 (12.4.3) - Administrator and operator log Enable auditing of changes to account identification and authentication mechanisms.	M	M
67	ISO 27001-2013 (9.4.1) - Information access restrictions Disable third-party accounts when not in use. <ul style="list-style-type: none"> <input type="checkbox"/> oweiner/Oscar Weiner <input type="checkbox"/> pfrattacelli/Paulo Frattacelli 	M	M
65	ISO 27001-2013 (8.2.2) - Labelling of information Implement a documented information labelling process.	M	M
62	ISO 27001-2013 (9.4.1) - Information access restrictions Investigate and determine if the users are former employees or third parties. Disable the accounts if they are no longer necessary.	M	L

Risk Score	Recommendation	Severity	Probability
	<input type="checkbox"/> Name: AD Jasper Last Login: 12/27/2017 7:42:51 AM <input type="checkbox"/> Name: ad keeler Last Login: <Unknown> <input type="checkbox"/> Name: ASPNET Last Login: <Unknown> <input type="checkbox"/> Name: Backup User Last Login: <Unknown> <input type="checkbox"/> Name: Backupsys Admin Last Login: <Unknown> <input type="checkbox"/> Name: Jayne Smyth Last Login: 12/14/2017 4:25:47 PM <input type="checkbox"/> Name: IUSR_DC12 Last Login: 10/12/2009 10:53:59 AM <input type="checkbox"/> Name: IUSR_STEINBRENNER Last Login: 4/11/2012 11:58:18 AM <input type="checkbox"/> Name: IWAM_DC12 Last Login: 4/30/2009 4:16:41 PM <input type="checkbox"/> Name: IWAM_STEINBRUNER Last Login: <Unknown> <input type="checkbox"/> Name: Horace Morris Last Login: 11/7/2017 6:51:14 AM <input type="checkbox"/> Name: FastAccts Service Account Last Login: 12/24/2009 12:01:30 PM		

Low Risk

Risk Score	Recommendation	Severity	Probability
50	ISO 27001-2013 (6.1.4) - Contact with special interest groups Maintain contact with special interest groups and document which individuals participate in the organisations.	L	L