Audit and Risk Management Committee

Date:	**Wednesday, 26 October 2022**
Time:	**6.00 p.m.**
Venue:	Wallasey Town Hall

Contact Officer: Joe D'Henin
Tel: 0151 691 8139
e-mail: josephdhenin@wirral.gov.uk
Website: http://www.wirral.gov.uk

Please note that public seating is limited therefore members of the public are encouraged to arrive in good time.

Wirral Council is fully committed to equalities and our obligations under The Equality Act 2010 and Public Sector Equality Duty. If you have any adjustments that would help you attend or participate at this meeting, please let us know as soon as possible and we would be happy to facilitate where possible. Please contact committeeservices@wirral.gov.uk

This meeting will be webcast at
https://wirral.public-i.tv/core/portal/home

AGENDA

11. ICT CONTINUITY CONTROLS (Pages 1 - 4)

Appendix A

The below graphics detail a snapshot, for a single minute, of Wirral Council's firewall logs, taken in March and October. The Firewall is Wirral Council's perimeter security only allowing authorised access. It can be viewed as the front door to Wirral Council's on-premise IT infrastructure.

March

The below graphics detail a snapshot of the Firewall logs taken in March.

Russia

#	▲Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	03-29 09:44	Russian Federation	45.155.204.188	193.161.4.136	RDP	Policy violation	deny
2	03-29 09:44	Russian Federation	91.240.118.19	193.161.4.182	tcp/3688	Policy violation	deny
3	03-29 09:44	Russian Federation	45.155.205.42	193.161.4.4	tcp/22246	Policy violation	deny
4	03-29 09:44	Russian Federation	91.240.118.19	193.161.4.165	tcp/3629	Policy violation	deny
5	03-29 09:44	Russian Federation	45.155.205.42	193.161.4.163	tcp/22290	Policy violation	deny
6	03-29 09:44	Russian Federation	91.240.118.43	193.161.4.96	tcp/3517	Policy violation	deny
7	03-29 09:44	Russian Federation	185.191.34.138	193.161.4.162	tcp/13531	Policy violation	deny
8	03-29 09:44	Russian Federation	45.155.205.46	193.161.4.88	tcp/23268	Policy violation	deny
9	03-29 09:44	Russian Federation	91.240.118.19	193.161.4.127	tcp/3671	Policy violation	deny
10	03-29 09:44	Russian Federation	45.146.165.165	193.161.4.127	MiNet Call Control	Policy violation	deny
11	03-29 09:44	Russian Federation	45.155.205.45	193.161.4.124	tcp/23132	Policy violation	deny
12	03-29 09:44	Russian Federation	185.191.34.132	193.161.4.136	tcp/10021	Policy violation	deny
13	03-29 09:44	Russian Federation	193.3.19.33	193.161.4.105	UDP 1024-3024	Policy violation	deny
14	03-29 09:44	Russian Federation	45.155.204.63	193.161.4.152	tcp/9580	Policy violation	deny
15	03-29 09:44	Russian Federation	45.146.165.165	193.161.4.53	MiNet Call Control	Policy violation	deny
16	03-29 09:44	Russian Federation	45.155.205.46	193.161.4.88	tcp/23266	Policy violation	deny
17	03-29 09:44	Russian Federation	45.155.205.45	193.161.4.144	tcp/23224	Policy violation	deny
18	03-29 09:44	Russian Federation	45.155.205.45	193.161.4.168	tcp/23131	Policy violation	deny
19	03-29 09:44	Russian Federation	45.146.165.165	193.161.4.21	MiNet Call Control	Policy violation	deny
20	03-29 09:44	Russian Federation	45.146.165.165	193.161.4.32	MiNet Call Control	Policy violation	deny

China

#	▲Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	03-29 09:44	China	101.132.101.109	193.161.4.192	TELNET	Policy violation	deny
2	03-29 09:44	China	118.182.119.156	193.161.4.44	tcp/808	Policy violation	deny
3	03-29 09:44	China	219.145.144.59	193.161.4.16	tcp/56476	Policy violation	deny
4	03-29 09:44	China	103.36.210.6	193.161.4.192	tcp/24044	Policy violation	deny
5	03-29 09:44	China	183.136.226.3	193.161.4.173	HTTPS	Policy violation	deny
6	03-29 09:44	China	103.36.210.6	193.161.4.212	tcp/24044	Policy violation	deny
7	03-29 09:44	China	202.98.215.103	193.161.4.154	tcp/15071	Policy violation	deny
8	03-29 09:44	China	60.2.37.70	193.161.4.129	TELNET	Policy violation	deny
9	03-29 09:44	China	182.43.242.243	193.161.4.211	tcp/7001	Policy violation	deny
10	03-29 09:44	China	62.234.130.84	193.161.4.157	UDP 1024-3024	Policy violation	deny
11	03-29 09:44	China	183.195.241.226	193.161.4.179	udp/8083	Policy violation	deny
12	03-29 09:44	China	103.45.131.10	193.161.4.141	udp/8000	Policy violation	deny
13	03-29 09:44	China	62.234.130.84	193.161.4.182	UDP 1024-3024	Policy violation	deny
14	03-29 09:44	China	125.111.252.246	193.161.4.212	tcp/54522	Policy violation	deny
15	03-29 09:44	China	101.132.101.109	193.161.4.192	TELNET	Policy violation	deny
16	03-29 09:44	China	60.169.17.6	193.161.4.182	TELNET	Policy violation	deny
17	03-29 09:44	China	62.234.130.84	193.161.4.102	UDP 1024-3024	Policy violation	deny
18	03-29 09:44	China	109.244.18.237	193.161.4.220	TELNET	Policy violation	deny
19	03-29 09:44	China	101.200.166.251	193.161.4.143	TELNET	Policy violation	deny
20	03-29 09:44	China	60.218.96.108	193.161.4.68	TELNET	Policy violation	deny

Korea

#	▲Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.12	tcp/53022	Policy violation	deny
2	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.110	tcp/53022	Policy violation	deny
3	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.49	tcp/53022	Policy violation	deny
4	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.21	tcp/53022	Policy violation	deny
5	03-29 09:44	Korea, Republic...	122.34.211.185	193.161.4.200	TELNET	Policy violation	deny
6	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.40	tcp/53022	Policy violation	deny
7	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.32	tcp/53022	Policy violation	deny
8	03-29 09:44	Korea, Republic...	61.72.255.26	193.161.4.83	tcp/53022	Policy violation	deny
9	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.18	tcp/53022	Policy violation	deny
10	03-29 09:45	Korea, Republic...	112.161.107.244	193.161.4.165	HTTP	Policy violation	deny
11	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.51	tcp/53022	Policy violation	deny
12	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.96	tcp/53022	Policy violation	deny
13	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.48	tcp/53022	Policy violation	deny
14	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.44	tcp/53022	Policy violation	deny
15	03-29 09:45	Korea, Republic...	112.212.33.231	193.161.4.220	TELNET	Policy violation	deny
16	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.17	tcp/53022	Policy violation	deny
17	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.88	tcp/53022	Policy violation	deny
18	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.74	tcp/53022	Policy violation	deny
19	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.16	tcp/53022	Policy violation	deny
20	03-29 09:45	Korea, Republic...	61.72.255.26	193.161.4.93	tcp/53022	Policy violation	deny

October

The below graphics detail a snapshot of the Firewall logs taken in October.

Russia

#	▼Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	10-24 09:54	Russian Federation	176.111.174.97	193.161.4.189	UDP 1024-3024	Policy violation	deny
2	10-24 09:54	Russian Federation	92.255.85.202	193.161.4.173	UDP 1024-3024	Policy violation	deny
3	10-24 09:54	Russian Federation	193.201.9.150	193.161.4.83	tcp/30007	Policy violation	deny
4	10-24 09:54	Russian Federation	193.201.9.150	193.161.4.83	tcp/30007	Policy violation	deny
5	10-24 09:54	Russian Federation	176.111.174.105	193.161.4.70	UDP 1024-3024	Policy violation	deny
6	10-24 09:54	Russian Federation	193.201.9.150	193.161.4.83	tcp/30007	Policy violation	deny
7	10-24 09:54	Russian Federation	176.111.174.80	193.161.4.66	UDP 1024-3024	Policy violation	deny
8	10-24 09:54	Russian Federation	185.122.204.244	193.161.4.170	tcp/3362	Policy violation	deny
9	10-24 09:54	Russian Federation	176.111.174.86	193.161.4.102	UDP 1024-3024	Policy violation	deny
10	10-24 09:54	Russian Federation	176.111.174.82	193.161.4.142	5500-5800/tcp	Policy violation	deny
11	10-24 09:54	Russian Federation	176.111.174.84	193.161.4.68	tcp/33383	Policy violation	deny
12	10-24 09:53	Russian Federation	176.111.174.84	193.161.4.44	tcp/33398	Policy violation	deny
13	10-24 09:53	Russian Federation	176.209.134.54	193.161.4.21	1433/tcp	Policy violation	deny
14	10-24 09:53	Russian Federation	92.255.85.202	193.161.4.173	UDP 1024-3024	Policy violation	deny
15	10-24 09:53	Russian Federation	176.111.174.85	193.161.4.83	UDP 1024-3024	Policy violation	deny
16	10-24 09:53	Russian Federation	176.111.174.88	193.161.4.152	UDP 1024-3024	Policy violation	deny
17	10-24 09:53	Russian Federation	176.111.174.105	193.161.4.190	UDP 1024-3024	Policy violation	deny
18	10-24 09:53	Russian Federation	91.204.139.118	193.161.4.106	SMB	Policy violation	deny
19	10-24 09:53	Russian Federation	92.255.85.202	193.161.4.136	UDP 1024-3024	Policy violation	deny
20	10-24 09:53	Russian Federation	176.111.174.81	193.161.4.16	tcp/3380	Policy violation	deny

China

#	▼Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	10-24 09:54	China	180.116.124.2	193.161.4.180	TELNET	Policy violation	deny
2	10-24 09:54	China	180.116.124.2	193.161.4.180	TELNET	Policy violation	deny
3	10-24 09:54	China	123.172.50.126	193.161.4.75	UDP 1024-3024	Policy violation	deny
4	10-24 09:54	China	123.172.50.126	193.161.4.75	UDP 1024-3024	Policy violation	deny
5	10-24 09:54	China	125.123.196.24	193.161.4.89	SMB	Policy violation	deny
6	10-24 09:54	China	115.59.251.19	193.161.4.235	TELNET	Policy violation	deny
7	10-24 09:54	China	54.223.113.30	193.161.4.88	PING	Policy violation	deny
8	10-24 09:54	China	101.200.78.47	193.161.4.175	UDP 1024-3024	Policy violation	deny
9	10-24 09:53	China	47.110.134.117	193.161.4.129	tcp/6379	Policy violation	deny
10	10-24 09:53	China	47.110.134.117	193.161.4.44	tcp/6379	Policy violation	deny
11	10-24 09:53	China	47.110.134.117	193.161.4.16	tcp/6379	Policy violation	deny
12	10-24 09:53	China	47.110.134.117	193.161.4.173	tcp/6379	Policy violation	deny
13	10-24 09:53	China	47.110.134.117	193.161.4.220	tcp/6379	Policy violation	deny
14	10-24 09:53	China	47.110.134.117	193.161.4.4	tcp/6379	Policy violation	deny
15	10-24 09:53	China	47.110.134.117	193.161.4.234	tcp/6379	Policy violation	deny
16	10-24 09:53	China	47.110.134.117	193.161.4.12	tcp/6379	Policy violation	deny
17	10-24 09:53	China	47.110.134.117	193.161.4.152	tcp/6379	Policy violation	deny
18	10-24 09:53	China	47.110.134.117	193.161.4.11	tcp/6379	Policy violation	deny
19	10-24 09:53	China	47.110.134.117	193.161.4.93	tcp/6379	Policy violation	deny
20	10-24 09:53	China	47.110.134.117	193.161.4.211	tcp/6379	Policy violation	deny

Korea

#	▼Date/Time	Source Country	Source IP	Destination IP	Service	Action	Firewall Action
1	10-24 09:54	Korea, Republic of	222.104.115.93	193.161.4.12	TELNET	Policy violation	deny
2	10-24 09:54	Korea, Republic of	222.100.4.138	193.161.4.197	TELNET	Policy violation	deny
3	10-24 09:54	Korea, Republic of	118.216.158.25	193.161.4.124	TELNET	Policy violation	deny
4	10-24 09:53	Korea, Republic of	112.167.23.61	193.161.4.198	TELNET	Policy violation	deny
5	10-24 09:53	Korea, Republic of	1.253.174.206	193.161.4.17	TELNET	Policy violation	deny
6	10-24 09:53	Korea, Republic of	112.162.62.10	193.161.4.127	TELNET	Policy violation	deny
7	10-24 09:53	Korea, Republic of	220.125.73.164	193.161.4.12	TELNET	Policy violation	deny
8	10-24 09:53	Korea, Republic of	183.106.186.47	193.161.4.231	TELNET	Policy violation	deny
9	10-24 09:52	Korea, Republic of	121.140.14.98	193.161.4.188	TELNET	Policy violation	deny
10	10-24 09:52	Korea, Republic of	119.202.130.96	193.161.4.140	TELNET	Policy violation	deny
11	10-24 09:52	Korea, Republic of	110.13.172.126	193.161.4.111	TELNET	Policy violation	deny
12	10-24 09:52	Korea, Republic of	121.190.56.114	193.161.4.44	TELNET	Policy violation	deny
13	10-24 09:52	Korea, Republic of	221.141.3.123	193.161.4.175	1433/tcp	Policy violation	deny
14	10-24 09:52	Korea, Republic of	221.141.3.123	193.161.4.175	1433/tcp	Policy violation	deny
15	10-24 09:52	Korea, Republic of	211.48.189.147	193.161.4.60	TELNET	Policy violation	deny
16	10-24 09:52	Korea, Republic of	180.182.245.134	193.161.4.198	8080/tcp	Policy violation	deny
17	10-24 09:51	Korea, Republic of	121.178.139.136	193.161.4.108	TELNET	Policy violation	deny
18	10-24 09:51	Korea, Republic of	221.164.165.131	193.161.4.174	TELNET	Policy violation	deny
19	10-24 09:51	Korea, Republic of	59.8.203.232	193.161.4.12	tcp/37215	Policy violation	deny
20	10-24 09:51	Korea, Republic of	121.151.205.83	193.161.4.105	TELNET	Policy violation	deny

This page is intentionally left blank