

Qamar Sheikh

Security and Infrastructure Director

qamar@visav.co.uk



Space Data Centre

- PASF
- ISO 27001 / 9001
- Cyber Essentials Plus
- G-Cloud
- Tier III
- Arranging visits summer 2021



Data and Security Document

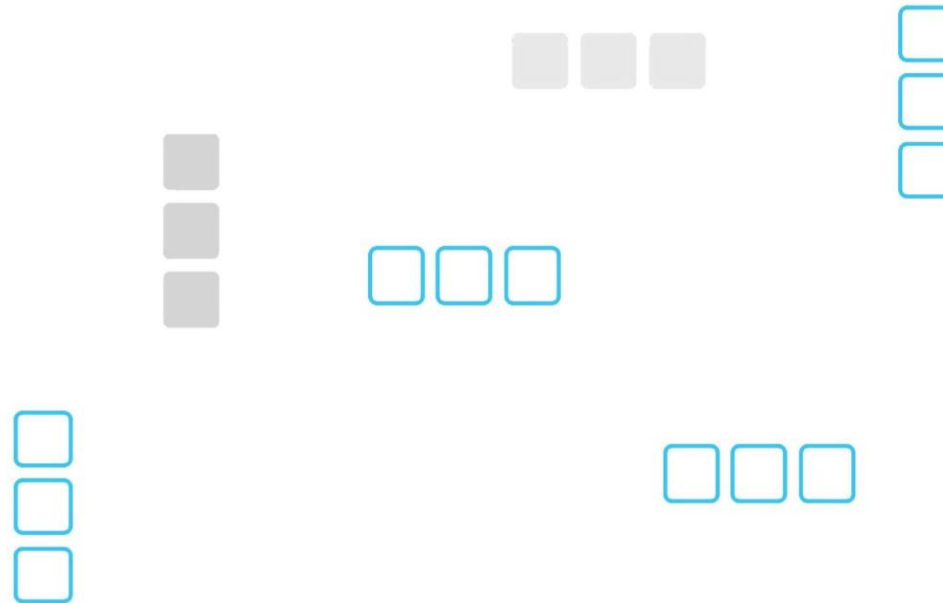
- <https://visav ltd.zendesk.com/hc/en-gb/articles/209034405-Security-and-Data-Compliance>
- www.neighbourhoodalert.co.uk/accreditations



Security Data Compliance V2.3:

Neighbourhood Alert Platform
Security , Data Protection, Resilience and Disaster Recovery .

January 2021



Contents

Contents

Staff Vetting	6
1. Hosting pertinent points:	6
2. System Schematics / Hardware / Software Overview	8
3. Security of the system is of paramount importance	10
4. Disaster Recovery and Backups	12
5. Service Level Agreement	13
Approved notification methods	13
Response times	13
6. Website DDA compliance and W3C accessibility guidelines	14
7. Web browser compatibility	15
End user password management	20
The "Full user editor"	21
Audit trail: sent messages	23
Message history audit	23
Adherence to the obligations of Data Protection	28
Lawfulness, fairness, and transparency	28
Purpose limitation	29
Data minimisation	29
Accuracy	29
Storage Limitation	30
Integrity and confidentiality (security)	30
Accountability	31
How VISAV Ltd Implement the NCSC Cloud Security Principles	32
Data in transit protection	32
Asset protection and resilience	32
a. Physical resilience & availability	32
b. Data Centre security	33
c. Data at rest protection	33
d. Data Sanitisation	33
e. Equipment disposal	33
f. Physical resilience & availability	33
Separation between users	34
Governance framework	34
Operational Security	34

Secure	user	management	
			37
e. Authentication of consumers to management interfaces and within			
Support		channels	
			37
f. Separation and access control within management interfaces			
Identity	and	authentication	
			38
External interface			
protection		Secure service	
administration		Audit	
information provision for users			39
Secure	use	of	the
service			39

Introduction

Overview

The Neighbourhood Alert system (Alert) is a secure, online, partnership-based community messaging facility. Alert enables twenty-three UK Police Forces to work seamlessly with other voluntary and public sector partners such as Neighbourhood Watch, the Local Authority, Fire & Rescue Service and the Office of the Police Commissioner (OPCC) as well as bordering Police Forces. The system provides the facility for citizens to self-register, log in and securely update their own details, including their interests and preferred method of communication.

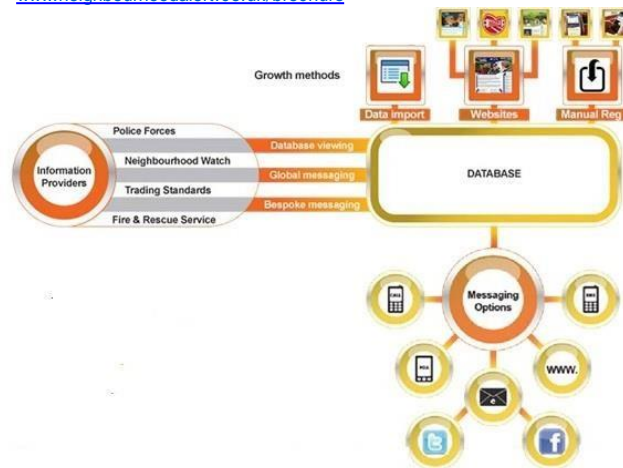
Alert has been custom built on Microsoft framework including Classic ASP and ASP.net since 2008 in close collaboration with several Police Forces and Neighbourhood Watch. It is a carefully controlled, permission led, geographically defined network of providers and end users. A new, entirely ASP.NET version is under construction and currently projected for launch by Q2 of 2021.

The system enables integration with multiple websites (Micro-sites). Citizens can join the database in several ways including registering via a local Micro-site, a National site (e.g. www.ourwatch.org.uk) or a police lead county portal or can be registered from Police handsets or standalone touch screen kiosks. Registration on any site within the Alert network provides a user with the ability to share their information with the licenced partners "Information providers".

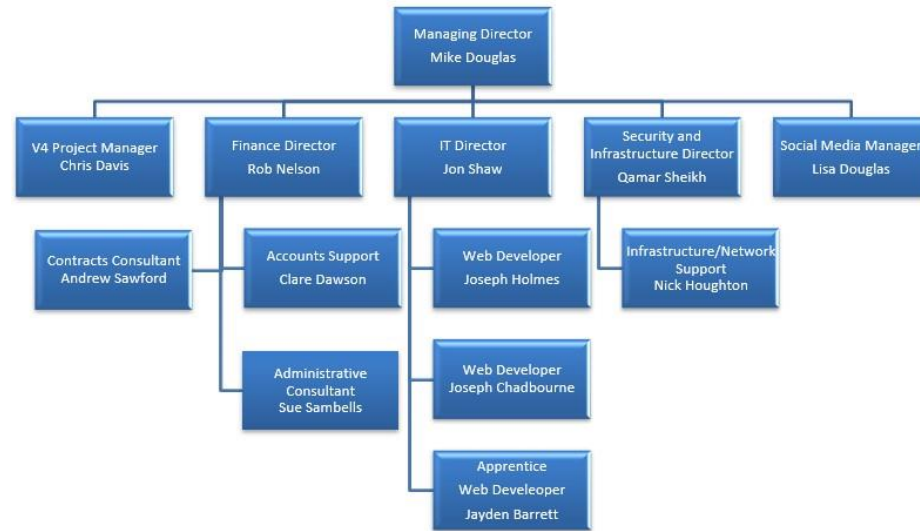
The system typically delivers between 8-11 million messages a month for over 3,000 police and other administrators to over 865,000 registered members with a forwarding reach of around 10 million people (*Figures as of October 2020*).

A feature overview can be downloaded from

www.neighbourhoodalert.co.uk/brochure



Organisational Chart



Staff Vetting

In 2017 Nottinghamshire Police evaluated that vetting of our staff was not required to host the system. This is mainly because VISAV Limited are joint Data Controllers for all data stored and responsible for the safeguarding of data managed and stored under our own ICO registration.

All staff are trained in data management, sign our NCSC, Cyber Essentials Plus accredited paperwork regarding data management and protection and are available for NPPV2 vetting by any Police Force that requires it. Jon Shaw and Mike Douglas are vetted to NPPV2 (Full) by West Midlands Police and will continue to maintain that minimum level of vetting.

Vetting of the above can be corroborated by:

Helen Thompson
Communications Manager
Corporate Communications
West Midlands Police
helen.thompson@west-midlands.pnn.police.uk
Tel: 0739 286 3228
Direct Dial: 0121 626 5858

1. **Hosting pertinent points:**

1. Our own equipment is co-located within Space Data Centres, Rani Drive, Nottingham, NG5 1RF, England. <https://www.spacedatacentres.co.uk> ISO27001 Cert No. 10250
2. VISAV run monthly external App-Check web application pen-tests on core Alert sites and internal/external Nessus scans weekly
3. Internal vulnerability/patch/advanced and network scanning is carried out weekly with remediation at the Datacentre and VISAV Head Office.
4. [VISAV is registered with the ICO No Z8862537 \(from Dec 2004\)](#)
5. A **PASF** (Police Approved Secure Facility) audit was performed on 24th April 2019 by Paul Ryan (Information Security Officer) Nottinghamshire Police at the Data Centre and at our Head Office on 24th May 2019. The results are now accessible on the on Police ICT Company Knowledge Hub.
6. As part of the PASF audit an **I.T. Health Check** (ITHC) was conducted in September 2019 at the Datacentre with external web application pen-test by a CREST approved provider (report is accessible on Police ICT Company Knowledge Hub)



7. An external web application pen test was performed by West Midlands Police in February 2019.
8. The hosting environment is **ISO27001** Certificate No 10250-ISMS-001, valid until 18 April 2022 (view [here](#).) and 9001 ISO Certificate No 10250-QMS-001.
9. The entire system has been evaluated by our case worker at the ICO, post May 2018 to assure its current and compliance to UK GDPR and Data Protection 2018/2020 regulations.
10. VISAV Limited have implemented a robust network infrastructure in accordance with NCSC GPG8 and GPG13 and have been audited to Cyber Essentials Plus using IASME accredited to its Gold standard using an external assessor, and to ISO9001:2015 & ISO14001:2015- view our certifications [here](#).



11. Information/Cyber Security is a board level responsibility and collectively the whole board is responsible for its implementation throughout the organisation as our Cyber Risk Assessment extends beyond IT infrastructure and into all aspects of our culture.

2. System Schematics / Hardware / Software Overview

The Neighbourhood Alert system servers are in Nottingham, within a highly resilient (ISO27001) accredited tier 3+ data centre with optimised temperature control utilising hot/cold aisle containment, with resilient connectivity and power.

Bandwidth:

Our current system is used by twenty-five plus Police forces, National Neighbourhood Watch, several local authorities and Fire & Rescue services. We facilitate 8-11 million messages a month sent by over 3000 administrators.

Our current/daily activity utilises around 20% of our contracted bandwidth, therefore during high demand situations (floods, snow etc), there is enough overhead capacity. We regularly review our bandwidth use and can increase our contracted bandwidth when required, at any time without impacting our systems. The economies of scale of the UK wide Alert system mean that we do not need to increase our licence costs as we increase this capacity.

Web Servers

We have a dedicated array of servers. Additional hardware and servers can be added to the array at any time that they are required, without impacting or interrupting existing systems. All web and mail servers are monitored internally and externally to ensure that they are operating well within operating parameters. Data storage is via SANs, comprising of SAS hot swappable drives within the secure environment which can be expanded whenever required.

Message delivery

The voice, text and email delivery mechanisms within the Neighbourhood Alert system run well within our operating parameters. Where systems are outsourced and third-party suppliers are used for delivery, robust SLAs are in place to ensure that third party systems are as reliable as the Alert system. Each message delivery system can scale-up according to short and long-term demand increases.

Save wastage at source

A key element often missed when considering increased message requirements is the intelligence elements of the message system itself. We prevent a great deal of wasted message bandwidth and cost by providing systems that reduce wasted messages caused by:

- Invalid email addresses
- Dead phone numbers
- Irrelevant, unwanted message types
- Duplicated messages (e.g., emailing and texting the same messages)
- Multiple accounts receiving the same message

Each outgoing message is given a priority level (1-5) which influences the capacity used to deliver it. The following diagram and explanation illustrate the three main message delivery methods and how they can be up scaled to manage both instant and long-term demand.

Email servers

Email is delivered using our own dedicated fail-over/round robin SonicWall hardware email endpoints. Queues, reputation and external mail server backlogs are monitored and managed 24/7. During short term high demand, (emergency/floods etc) the clustered system spreads the load between the perimeter email devices.

This huge capacity, bulk email system could be further enhanced by adding additional data centres to the current cluster if required. Current use is less than 50% of our available email delivery resource and we estimate will be well within acceptable parameters for the next two years but can be increased quickly if required

Text messages

Alert uses only premium UK based multi-location message centres. The infrastructure delivers SMS using various preferred routes into each provider's network message delivery centres. Messages are then delivered to the recipient's handset as fast as the network's own systems allow.

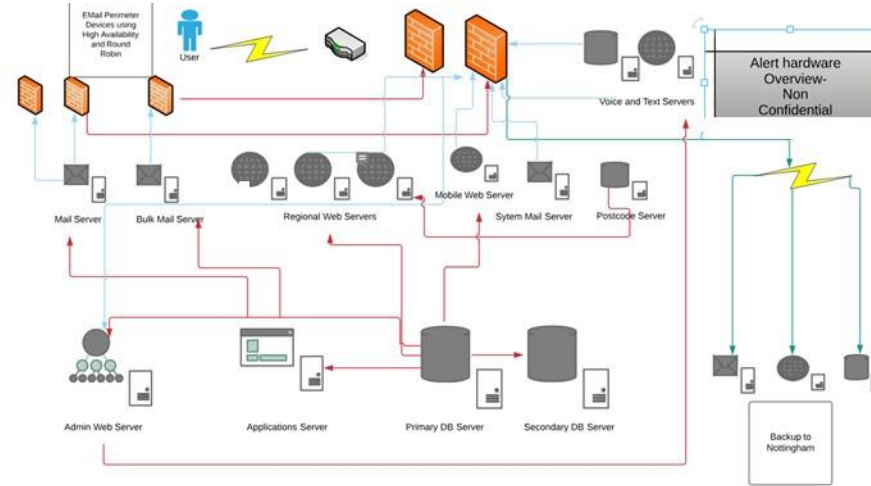
This one-to-one messaging procedure is the quickest, most effective / reliable way to deliver SMS messages without the delays associated with non-premium one-to-many bulk broadcast messaging services. Messages enter the mobile network via a robust network with huge capacity far beyond any level that we are projected to reach in the next five years.

Voice calls

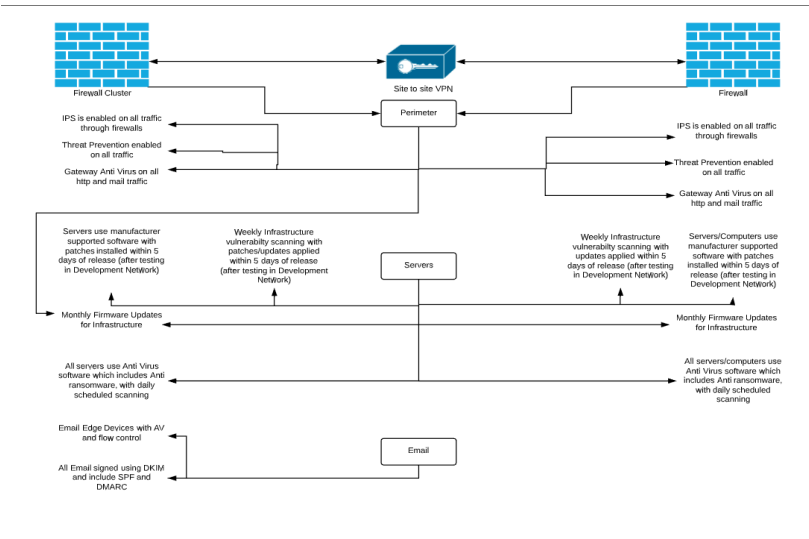
The Alert recorded voice call service connects directly to a highly robust digital call distribution service. This service operates out of three independent call centres in Manchester, Birmingham and London. During high demand or system failure, queued calls are passed to alternative systems.

The system supports multiple digital connections with capacity from 24 to 500 phone lines. The priority level and number of recipients selected for each voice message influences the number of lines used for distribution. These interactive voice response systems can be increased in capacity at any point should the demand necessitate it.

Hardware Overview Alert system



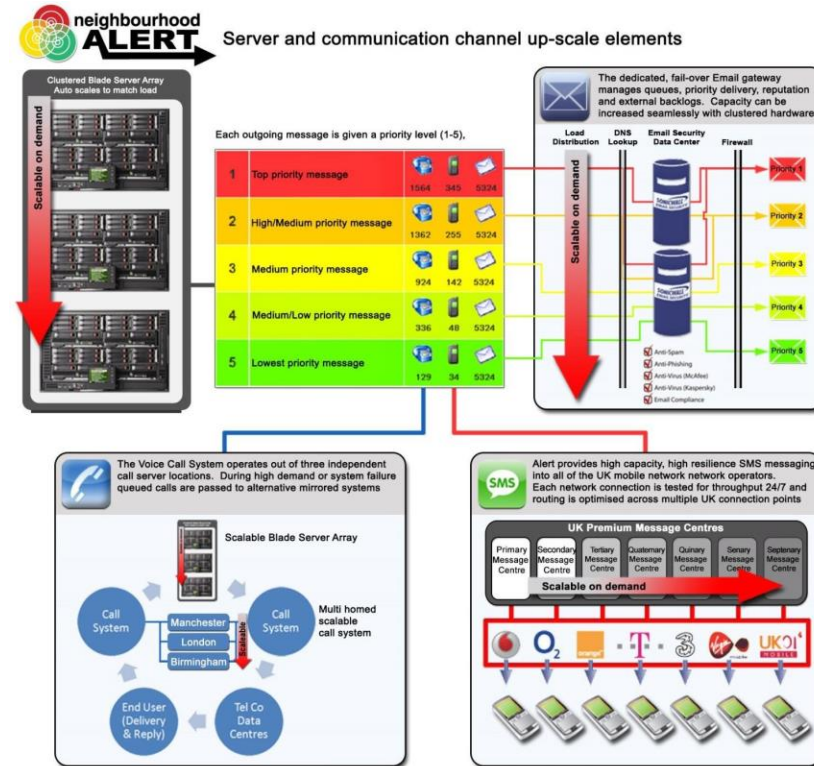
Security Overview



Summary

The hosting environment, mail, text and voice delivery hardware that can be provisioned for each new Force area can be allocated according to the capacity of each area and can be scaled up to match demand instantly if this spikes (see upscale diagram below). In addition, we have burstable internet, which will ensure additional guaranteed connectivity when required. We use Next Generation Firewalls which are CAPS approved.

Diagram illustrating the up-scale elements throughout the Alert system



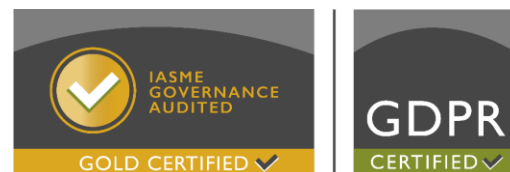
Our standard system provision per Force area has the capability to manage an area three times bigger than the average Force size and many users. For example, our largest Force so far is the Thames Valley system which runs on our standard server allocation with 100,000 users and 1000 administrators and is currently using less than 10% of its available resources.

We use CAPS approved hardware to reinforce our perimeter security utilising the latest next generation firewall technologies

<https://iasme.co.uk/iasme-governance/iasme-governance-audited/>

The procurement teams of many large companies will accept the **IASME Governance Audited standard as independent confirmation of good information and cyber security practice.** This is **extremely useful** when trying to win tenders and renew contracts, particularly where supplier requirements mention ISO 27001.

For example, **The Government of Jersey** is one organisation that has specified IASME Governance Standard within its security standards document.



4. Disaster Recovery and Backups

- A minimum of 7 database backups are made using different methods:
 - The live database is duplicated in real time through synchronous mirroring to a separate secure database server.
 - System and database backups are taken every 30 minutes to local SAN storage.
 - Incremental Alert data is backed up daily to offsite encrypted drives via a secure VPN connection to Nottingham
- All components in the data centre are fully redundant; there is no single point of failure.
- Multiple firewalls and switches with failover to ensure our perimeter services going offline, with plans to further this into clustered servers for our next web application V4
- Recovery would only be necessary if all servers of the same role are irrecoverable. Recovery can be made to available hardware or replacement hardware (we have a 2-hour onsite contract with a major hardware provider) using backups taken from one or multiple devices and locations.

In the extremely unlikely event that the main data centre should experience a total failure which was likely to last days, we have processes in place that would enable us to switch the system within a few hours to operate, albeit at reduced speed, from a permanently ready, redundant system hosted in our own steel encased server room in Nottingham.

5. Service Level Agreement

Please refer to "Schedule 3: VISAV Support Services for more information

Approved notification methods

Support tickets can be raised by :

1. **Emailing** support@neighbourhoodalert.co.uk at any time
2. Incoming calls to **telephone support (0115 8384630)** are turned into tickets by support staff if the matter relates to a service request.
3. **Out of office diverted calls** are recorded and automatically turned into support tickets, with text reminders to the on-call engineer; All senior staff are notified also over the Slack Messaging System.
4. Starting an **online chat request**. (Out Of Hours this will be turned into support tickets)

Response times

Response times are measured from the moment that you submit a support request via one of the approved notification methods above which tracks all issues from initial reporting to resolution.

VISAV is deemed to have responded when it has replied to the initial request. This may be in the form of an email, chat response or telephone call, to either provide a solution or request further information. Response times may depend on the priority of the item(s) affected and the severity of the issue. They are shown in this table:

Priorty y	Issue severity (see Severity levels section, below)	Response	Target Resolution Period
1	Urgent	Mon – Sun (8.30 am – 5.30 pm) 30 minutes Response	Mon – Sun (8.30 am – 5.30 pm) 4hr Resolution
2	High	Mon – Sun (8.30 am – 5.30 pm) 1hr Response	Mon – Sun (8.30 am – 5.30 pm) 8hr Resolution
3	Medium	Mon – Fri (8.30 am – 5.30 pm) 2hr Response	Mon – Fri (8.30 am – 5.30 pm) 1 day Resolution
4	Low	24-hour response Bespoke Work Requests via Practitioners Group	Next release of software /5 working day resolution

Response times apply during office working hours (8.30 am – 5.30 pm Monday to Friday) unless specified in this table, the issue is Urgent or High.

levels

The severity levels shown in the tables above are defined as follows:

- **Urgent:** Complete degradation — **all users and critical functions affected**. service completely unavailable.
- **High:** Significant degradation — **large number of users or critical functions** affected.
- **Medium:** Limited degradation — **limited number of users or functions** affected. Business processes can continue.
- **Low:** Small degradation — **few users or one user affected**. Business processes can continue. **Requests for enhancements** and system enhancements which require new software updates

6. Website DDA compliance and W3C accessibility guidelines

Alert sites are DDA compliant and meet W3C guidelines. They provide accessibility help, enabling computer users to make the most of the content and functionality on each site.

To help us make the sites a positive place for everyone, we use the Web Content Accessibility Guidelines (WCAG) 2.0 (<http://www.w3.org/TR/WCAG>). These guidelines explain how to make web content more accessible for people with disabilities, and user friendly for everyone.

The guidelines have three levels of accessibility (A, AA and AAA). We work to a minimum of Level A.

Example top row of an Alert site showing some Accessibility options



On Alert sites you can change the size of any text on the site by clicking on the 3 A's at the top of the screen. You can also access further explanation and support via the Accessibility link.

These are typical accessibility statements:

<https://www.stayintheknow.co.uk/accessibility>

<https://www.hampshirealert.co.uk/accessibility>

As Alert sites have a content managed element so you can upload your own content, and message content is also published to sites when appropriate, you will need to ensure that your content is accessible.

VISAV provides guidelines and training to ensure that the compliance is maintained. We check the site with automated compliance checking software at least once every three months and we provide a free fault reporting system and phone number for end users to report any issues.
























The Alert infrastructure enables many guidelines such as use of style sheets to control presentation to ensure that specialised reading software works effectively.




Our content management system (CMS) enables adherence to the key DDA guidelines with simple to use tools; these elements include tools to provide a text equivalent to non-text elements (e.g. "alt" or "Title" text in the image content).

CMS training reinforces these and other DDA requirements. Any items that are highlighted that fall outside of the compliance guidelines will be rectified without charge.

7. Web browser compatibility

We can test our sites for compatibility in over 700 web browsers (using www.browserstack.com),

Windows 10	 18.17.16.15 insider preview  11	 71.70.69.68.67.66.65.64.63.62. 61.60.59.58.57.56.55.54.53.52. 51.50.49.48.47.46.45.44.43.42. 41.40.39.38.37	 69.62.61.60.59.58.57.56.55.54. 53.52.51.50.49.48.47.46.45.44. 43.42.41.40.39.38.37.36.35.34. 33.32	
Windows 8.1	 11	 71.70.69.68.67.66.65.64.63.62. 61.60.59.58.57.56.55.54.53.52. 51.50.49.48.47.46.45.44.43.42. 41.40.39.38.37.36.35.34.33.32. 31.30.29.28.27.26.25.24.23.22	 69.62.61.60.59.58.57.56.55.54. 53.52.51.50.49.48.47.46.45.44. 43.42.41.40.39.38.37.36.35.34. 33.32.31.30.29.28.27.26.25.24. 23.22.21.20.19.18.17.16	 12.16.12.15.12.14.12.1.12
Windows 8	 10	 71.70.69.68.67.66.65.64.63.62. 61.60.59.58.57.56.55.54.53.52. 51.50.49.48.47.46.45.44.43.42. 41.40.39.38.37.36.35.34.33.32. 31.30.29.28.27.26.25.24.23.22	 69.62.61.60.59.58.57.56.55.54. 53.52.51.50.49.48.47.46.45.44. 43.42.41.40.39.38.37.36.35.34. 33.32.31.30.29.28.27.26.25.24. 23.22.21.20.19.18.17.16	 12.16.12.15.12.14.12.1.12
Windows 7	 11.10.9.8	 71.70.69.68.67.66.65.64.63.62. 61.60.59.58.57.56.55.54.53.52. 51.50.49.48.47.46.45.44.43.42. 41.40.39.38.37.36.35.34.33.32. 31.30.29.28.27.26.25.24.23.22. 21.20.19.18.17.16.15.14	 69.62.61.60.59.58.57.56.55.54. 53.52.51.50.49.48.47.46.45.44. 43.42.41.40.39.38.37.36.35.34. 33.32.31.30.29.28.27.26.25.24. 23.22.21.20.19.18.17.16.15.14. 13.12.11.10.9.8.7.6.5.4.3.6	 12.16.12.15.12.14.12.1.11.6
Windows XP	 7.6	 49.48.47.46.45.44.43.42.41.40. 39.38.37.36.35.34.33.32.31.30. 29.28.27.26.25.24.23.22.21.20. 19.18.17.16.15.14	 47.46.45.44.43.42.41.40.39.37. 36.35.34.33.32.31.30.29.28.27. 26.25.24.23.22.21.20.19.18.17. 16.15.14.13.12.11.10.9.8.7.6.5.4. 3.8	 12.16.12.15.12.14.12.1.11.6
Mac OS X Catalina	 13.1	 71.70.69.68.67.66.65.64.63.62. 61.60.59.58.57.56.55.54.53.52. 51.50.49.48.47.46.45.44.43.42. 41.40.39	 69.62.61.60.59.58.57.56.55.54. 53.52.51.50.49.48.47.46.45.44. 43.42.41.40.39.38.37.36.35.34. 33.32.31.30.29.28.27.26.25.24. 23.22.21.20.19.18.17.16.15.14	

 iOS	iPhone		iPad			
	<div><div>iPhone 7 (v10)</div><div>iPhone SE (v11)</div><div>iPhone 6 (v11)</div><div>iPhone 6S Plus (v11)</div><div>iPhone 6S (v11)</div><div>iPhone 8 Plus (v11)</div><div>iPhone 8 (v11)</div><div>iPhone X (v11)</div><div>iPhone 6S (v12)</div><div>iPhone 7 (v12)</div></div>	<div><div>iPhone 8 (v12)</div><div>iPhone XR (v12)</div><div>iPhone XS Max (v12)</div><div>iPhone XS (v12)</div><div>iPhone 4S (v5.1)</div><div>iPhone 5 (v6.0)</div><div>iPhone 4S (v6.0)</div><div>iPhone 5S (v7.0)</div><div>iPhone 6 Plus (v8.3)</div><div>iPhone 6 (v8.3)</div></div>	<div><div>iPad 5th (v11)</div><div>iPad 6th (v11)</div><div>iPad Mini 4 (v11)</div><div>iPad Pro 12.9 2017 (v11)</div><div>iPad Pro 9.7 2016 (v11)</div><div>iPad Air 2019 (v12)</div><div>iPad Mini 2019 (v12)</div><div>iPad Pro 11 2018 (v12)</div></div>	<div><div>iPad Pro 12.9 2018 (v12)</div><div>iPad 2 (v5.0)</div><div>iPad 3rd (v5.1)</div><div>iPad 3rd (v6.0)</div><div>iPad Mini (v7.0)</div><div>iPad 4th (v7.0)</div><div>iPad Air (v8.3)</div><div>iPad Mini 2 (v8.3)</div></div>		
 Android	Samsung		Google	Motorola	Amazon	HTC
	<div><div>Galaxy Tab 4 (v4.4)</div><div>Galaxy Tab S3 (v7.0)</div><div>Galaxy Tab S3 (v8.0)</div><div>Galaxy Tab S4</div><div>Galaxy Tab S5e</div><div>Galaxy Note 4 (v4.4)</div><div>Galaxy S6</div><div>Galaxy Note 4 (v6.0)</div><div>Galaxy S7</div><div>Galaxy S8</div><div>Galaxy S8 Plus (v7.0)</div><div>Galaxy A8</div><div>Galaxy Note 8</div><div>Galaxy S9</div><div>Galaxy S9 Plus (v8.0)</div><div>Galaxy Note 9</div></div>	<div><div>Galaxy S10 Plus</div><div>Galaxy S10e</div><div>Galaxy S8 Plus (v9.0)</div><div>Galaxy S9 Plus (v9.0)</div><div>Galaxy Note</div><div>Galaxy Note 10.1</div><div>Galaxy Note 2</div><div>Galaxy Note 3</div><div>Galaxy Tab 4 (v4.4)</div><div>Galaxy S5 Mini</div><div>Galaxy Tab 2</div><div>Galaxy S2</div><div>Galaxy S3</div><div>Galaxy S4</div><div>Galaxy S5</div></div>	<div><div>Nexus 5 (v4.4)</div><div>Nexus 6 (v5.0)</div><div>Nexus 6 (v6.0)</div><div>Pixel (v7.1)</div><div>Pixel (v8.0)</div><div>Pixel 2 (v8.0)</div><div>Pixel 2 (v9.0)</div><div>Pixel 3</div><div>Pixel 3 XL</div><div>Nexus</div><div>Nexus 4</div><div>Nexus 5 (v5.0)</div><div>Nexus 6 (v5.0)</div><div>Nexus 7</div><div>Nexus 9</div></div>	<div><div>Moto X 2nd Gen (v5.0)</div><div>Moto X 2nd Gen (v6.0)</div><div>Razr Maxx HD</div><div>Droid Razr</div><div>Razr</div></div>	<div><div>Kindle Fire HDX 7</div><div>Kindle Fire HD 8.9</div><div>Kindle Fire 2</div></div>	<div><div>Wildfire</div><div>One X</div><div>One M8</div></div>
 Windows 10	<div><div>insider preview</div><div>18 17 16 15</div><div>11</div></div>	<div><div>71 70 69 68 67 66 65 64 63</div><div>62 61 60 59 58 57 56 55 54</div><div>53 52 51 50 49 48 47 46 45</div><div>44 43 42 41 40 39 38 37</div></div>	<div><div>63 62 61 60 59 58 57 56 55</div><div>54 53 52 51 50 49 48 47 46</div><div>45 44 43 42 41 40 39 38 37</div><div>36 35 34 33 32</div></div>			
 Windows 8.1	<div><div>11</div></div>	<div><div>71 70 69 68 67 66 65 64 63</div><div>62 61 60 59 58 57 56 55 54</div><div>53 52 51 50 49 48 47 46 45</div><div>44 43 42 41 40 39 38 37 36</div><div>35 34 33 32 31 30 29 28 27</div><div>26 25 24 23 22</div></div>	<div><div>63 62 61 60 59 58 57 56 55</div><div>54 53 52 51 50 49 48 47 46</div><div>45 44 43 42 41 40 39 38 37</div><div>36 35 34 33 32 31 30 29 28</div><div>27 26 25 24 23 22 21 20 19</div><div>18 17 16</div></div>	<div><div>12.16 12.15 12.14 12.1 12</div></div>		
 Windows 8	<div><div>10</div></div>	<div><div>71 70 69 68 67 66 65 64 63</div><div>62 61 60 59 58 57 56 55 54</div><div>53 52 51 50 49 48 47 46 45</div><div>44 43 42 41 40 39 38 37 36</div><div>35 34 33 32 31 30 29 28 27</div></div>	<div><div>63 62 61 60 59 58 57 56 55</div><div>54 53 52 51 50 49 48 47 46</div><div>45 44 43 42 41 40 39 38 37</div><div>36 35 34 33 32 31 30 29 28</div><div>27 26 25 24 23 22 21 20 19</div></div>	<div><div>12.16 12.15 12.14 12.1 12</div></div>		

Example screen shot of the selection of web browsers that each site is tested against.

We also ensure they are tested in the most secure version of each major manufacturer's supported web browser (Microsoft Edge, Apple Safari, Mozilla Firefox, Google Chrome). There are too many browsers to list but this will provide information to a typical compatibility test result for an Alert site. and ensure our SSL enabled websites use best practice

All new sites are thoroughly tested using the sites below before being launched and periodically afterwards

(<https://www.sslabs.com/sslttest/analyze.html?d=thamesvalleyalert.co.uk>).

(<https://securityheaders.com/?q=www.neighbourhoodalert.co.uk&hide=on&followRedirects=on>)

COMMERCIALLY SENSITIVE: NOT FOR FURTHER DISTRIBUTION
afterwards.

The sites are designed to HTML5 guidelines and W3c compliance

All sites are subject to both internal and external vulnerability scanning using a customised scanning templates which have been provided by our security partners to ensure standards are retained to Cyber Essential s PLUS.

Role based permission settings

Role name: PCSO [Edit](#) [View all admins of this role](#)

[illegible]

pg. 18

Additional access control by user type and area:

Specific administration access levels enable the close control of user data access per administrator by type of registered user. Access can be given to sections of the database based on user's profile, affiliations and memberships. Access can also, if required, over-ride standard geographic restrictions; types of specific access to groups include:

- 1) Neighbourhood Watch members
- 2) All users based on Beat areas
- 3) Business data, business types and user roles
- 4) Bespoke, configurable user sets
- 5) All Watch and Interest group membership
- 6) Restricted and/or hidden groups (victims, witnesses)

This high level of advanced permissions enables you, when required, to grant very specific access in order to make an administrator's use of the system highly flexible and purposeful. You may, for example, have a Key Individual Network of users who are all linked to the protection and safety of a specific resource (School, Forest area, Youth club, Search team etc) but the individual members live across a wide geographic area, well beyond the administrator's usual area of access (outside of beat, Neighbourhood or even Force area). Using these tools, these administrators would be able to see, map, manage and communicate with this KIN group wherever they were geographically based.

Administrator management:

Alert enables you to manage lots of administrators, in some cases thousands of them, all from one simple place. The list of administrators can be searched, and simple filters are available so you can find administrators by some of the main permissions they have access to.

Simple traffic light icons show you who has been active on the system and who is not so you can order the list of administrators by activity to quickly identify those who are not using the system.

The "Message sending mode" enables you to use this system to send a message to all administrators or specific ones based on role. This is ideal for updates, policies and guidance messages.

Search for an administrator

Search word:

Search

[Add a new administrator](#)

Use to communicate with all or some administrators {

Currently 235 registered administrators

Switch to message sending mode

 }

Filter by role and access

Administrator name **	Area covered **	Date added **							
Brian Adams	Hampshire	15/02/2015							Edit Reset Delete
Tony Anley	Sherwood & Hyson Green	14/07/2014							Edit Reset Delete
Jim Allen	North East	02/09/2014							Edit Reset Delete
Lynne Arch	Bedfordshire	21/03/2012							Edit Reset Delete

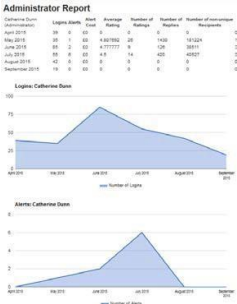
Track Active Admins

Monitor Administrator Activity

The "Report" link against each administrator generates a management report which highlights various performance figures for that administrator over the last six months.

Factors such as messages sent, ratings received, cost incurred, community reach compared to potential reach and number of new end-users added are all included.

These reports provide an instant comparison across administrators and an intuitive feel to how active and effective each administrator is being.



Self-Reset password

We also know that administrators can sometimes struggle with remembering passwords, so we make that as simple as possible to reset a password securely without the requirement to wait for an administrator to authorise it.

The password reset process is a secure, three tier system requiring the administrator to enter a memorable word before they can self-reset a password. We only allow a self-reset request to come from a .pnn/.police.uk email domain in order to prevent bogus attempts and denial of service attacks but allowing this level of self-help saves hours of delay, additional administrator time and reduces the frustration of the administrator when they are trying to log in.

Administrators can (as of Dec 16) request a password reset via a pin number that is sent to their (pre-entered) mobile number by text message.

Administrator account self-request

When you are rolling out the system to many administrators, we can assist by uploading a spreadsheet of details and auto creating the accounts for you. In some cases, though you may prefer to simply ask new administrators to request access to the system themselves. This may save you time in setting up the basic details and help you identify those of officers who feel they need access.

Basic details

Please enter the details below to request a mobile access account on the system.

First name *

Surname *

Group (Le Police or NNNNN) *

Rank or role (Le Sgt or coordinator) *

Area (Le North, best name or association) *

Email address *

Create account

To enable this, we have the ability for administrators with a pnn email address to complete a simple form and request access.

You are notified of these applications and can grant, decline or configure access easily.

End user password management

All user passwords are stored within the Alert database in an encrypted format; they cannot be viewed and changed by an administrator or even accessed by VISAV database managers/programmers. You cannot update or view a password, if an end user has forgotten their password, they will have to reset it by following a process triggered by a link from the website or that an administrator can send by email.

To make changes to a user's details the administrator should first log in to their account and go to the "search for a user" page. To find the person required the administrator can search by name, email address, telephone number, or postcode; once found, to access the member's details they simply click "view".

Example: Search for a user

1) Enter search term

2) Click "View"

A quick summary screen is then displayed which shows an overview of the member's information; as per the below screenshot this includes name, address and contact methods, any of which can be changed on this screen.

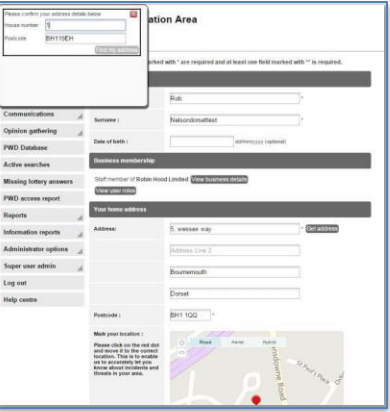
Example screenshot of user overview screen

More information can be accessed and updated by going to the user's "Full user editor"

The “Full user editor”

This main screen provides access to all the user's information and settings. A huge variety of configuration can be performed from this section if required. Most people do not require any configuration in this area as the standard settings are perfectly adequate and, if desired, users can log in to their own secure admin area and configure their own settings. This area is provided for the small number of users who require specific settings or passwords resetting.

Example: Full user editor, showing update address screen.



On this page you can see a map showing the location of the member's home address; when the address is amended as on the overview page, the map is automatically updated and the pin moved to show the new address (as shown in the below screenshot).

Example: updating a user's email address and email



If the email address is changed, the user is automatically sent an email to the new email address with a link to click to verify the new address.

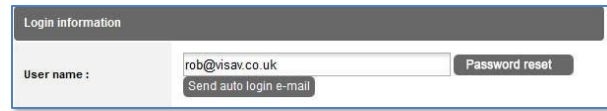
Example: Screenshot of other settings within the Full user editor



From this single page an administrator can access the user's message settings or add additional addresses for them (relatives, work address etc.)

They can also add or remove the user from groups, view the communications log or audit trail and add notes against the account.

Example screenshot, reset password section



The screenshot shows a web form titled "Login information". It contains a "User name :" label followed by a text input field containing "rob@visav.co.uk". Below the input field is a button labeled "Send auto login e-mail". To the right of the input field is a button labeled "Password reset".

The administrator can click the "password reset" button to trigger an email to be sent via the system to the user to enable them to answer a simple account question and then create a new password for their account (and thereby access it).






This section currently has an additional "auto login email" which is a back-up system for less technically able users who are struggling with the set-up password process. This button sends the user a link which, when clicked takes them straight to their account and logs them in automatically. Each link can only be used once and should be used sparingly as it grants access to a user's account. It is another example of a bespoke facility that has been added to the array of tools over the years to make this a practical facility for community messaging.

[Audit trail: sent messages](#)

The Message history section shows all outgoing messages, who sent them, when, to whom and what got delivered/failed. The following two sub answers provide further information on these reports.

[Message history audit](#)

The message history section continuously logs and stores all information regarding messages sent. You can search for any message and find every bit of information regarding who it was sent to, what the message was, what it cost, when it went etc. (senders' names redacted)

Alert #	Message sent	Sent by	Message	Emails	Voice	SMS	Message cost	Message details
355815	17/12/2020 09:26:00	[REDACTED]	Burglary - Belgrave Road Bingley	395	0	0	£0.00p	 
355814	17/12/2020 09:21:00	[REDACTED]	Emergency Help Guide - Midlothian	509	0	0	£0.00p	 
355813	17/12/2020 09:18:00	[REDACTED]	Criminal damage caused to fence panels on Yairborough Court in Barton upon Humber	131	0	0	£0.00p	 
355812	17/12/2020 09:17:00	[REDACTED]	Mole Valley Beat Bulletin Thurs 17th Dec 2020	1226	0	0	£0.00p	 
355811	17/12/2020 09:16:00	[REDACTED]	Garage Entered	68	0	0	£0.00p	 
355810	17/12/2020 09:13:00	[REDACTED]	Attempt burglary - Bankside Terrace	492	0	0	£0.00p	 
355809	17/12/2020 09:13:00	[REDACTED]	Owners Warning - Caravan Thefts	17998	0	0	£0.00p	 
355808	17/12/2020 09:07:00	[REDACTED]	Criminal Damage - Slim Avenue	4	0	0	£0.00p	 
355807	17/12/2020 09:06:00	[REDACTED]	Attempt burglary - Granby Drive	95	0	0	£0.00p	 
355806	17/12/2020 09:04:00	[REDACTED]	Vehicle Interference	6	0	0	£0.00p	 
355805	17/12/2020 09:00:00	[REDACTED]	Garage burglary - Pot House Road	409	0	0	£0.00p	 
355804	17/12/2020 08:59:00	[REDACTED]	Vehicle Interference - Parkview Road	2	0	0	£0.00p	 
355803	17/12/2020 08:54:00	[REDACTED]	Theft From Motor Vehicle	123	0	0	£0.00p	 
355802	17/12/2020 08:53:00	[REDACTED]	Arrest of the Ienton Burglar	378	0	0	£0.00p	 
355801	17/12/2020 08:52:00	[REDACTED]	Vehicle Crime	115	0	0	£0.00p	 

In addition to message sending audit reports, the system records every key action made by all administrators and end users. It date/time stamps all actions and records the IP address from which the user / administrator accessed the system; this information is stored for two years in a secure, encrypted form and can be queried by top-administrators at any time.

Example: Screenshot of audit trail report system

Audit trail for Neighbourhood Alert

Select audit trail entries to view : -- View all entries --

Filter results by

Filter by admin user :

Filter by date range :
(leave blank to view all)

enter dates as dd/mm/yyyy

- View all entries --
- Member logins
- Member login failures
- Password reminder requests
- Member account updates
- Scheme / patrol updates
- Information reports
- Message setting updates
- Skin preference updates
- Admin user logins
- Failed admin user logins
- Admin user updates
- Manual password reset
- Alert messages
- Information provider updates
- Group membership updates
- Community contacts group updates
- File uploads
- News articles
- Web page updates

Example: Audit trail sample showing actions and IP addresses

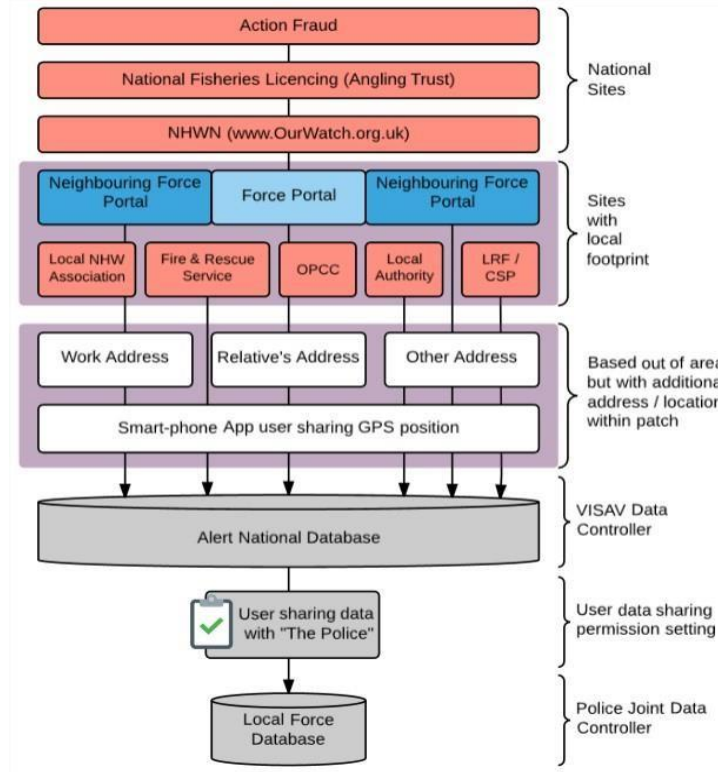
Entry date	Site name	Admin name	Member name	Action	IP
10/09/2015 16:13:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Roger Hartshorn	Member details updated by admin	62.232.34.130
10/09/2015 16:13:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Roger Hartshorn	Login reminder sent from admin	62.232.34.130
10/09/2015 15:09:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	N/A	Admin user logged in	62.232.34.130
10/09/2015 14:33:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	N/A	Admin user logged in	62.232.34.130
10/09/2015 14:28:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	N/A	Admin user logged in	62.232.34.130
10/09/2015 14:26:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Marie Fairweather	Member details updated by admin E-mail address updated from " " to " " @gmail.com" to " " @gmail.com"	62.232.34.130
10/09/2015 14:24:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Marie Fairweather	Member deleted by admin (Audit trail entry)	62.232.34.130
10/09/2015 14:24:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Marie Fairweather	Member deleted by admin	62.232.34.130
10/09/2015 14:24:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Marie Fairweather	User note added to account.	62.232.34.130
10/09/2015 13:54:00	Neighbourhood Alert	Mike Douglas (VISAV, Admin, Global)	Jaylani Nur	Member details updated by admin Postcode updated from 2 to 2 Close to 2 Close	62.232.34.130

9) Data Controller Status within the Neighbourhood Alert System

The Neighbourhood Alert system is a national database which is segmented into data sets based on geographic areas and each user's data sharing permissions. New users join the system via a wide range of websites, including national partner sites (Action Fraud, NHWN) and other optional local partners which are activated by agreement with the local Police force. All the web terms are the same and clearly define the Information Provider principles and data sharing implications.

This tested framework means that it does not matter which site a citizen joins. If a user lives or nominates an address within the geographic area you are authorized to see and they opt in to share their data with you, they join your database.

Combination of site joined, address and data consent, places a user in a local force database



Registered users can unsubscribe from any Information Provider at any time or leave the system altogether (if they are deleted).

Registration Process

VISAV Ltd have (in conjunction with the DEV Board) completely updated the registration process to include specific and lawful opt-ins as below:
(for www.neighbourhoodalert.co.uk)

Who can send you messages?

Select below the Information Providers that you want to share your data with and receive messages from (this can be changed at any time later).

- ☐ Fire & Rescue Service * [More info](#)
- ☐ Get Safe Online [More info](#)
- ☐ Local Authority * [More info](#)
- ☐ Neighbourhood Watch * [More info](#)
- ☐ Office of the Police & Crime Commissioner * [More info](#)
- ☐ SGN (Gas Emergency Service) * [More info](#)
- ☐ The Police * [More info](#)
- ☐ Action Fraud (NFIB) [More info](#)

* Suggested selections for a basic service.

I consent to share my data as defined above for the purposes of receiving information in accordance with the website [terms and conditions](#) and [privacy policy](#). I also understand that VISAV Ltd will have access to my information in order to manage the system and send important system updates to me.

The "default" providers are now suggested with a red asterisk and not automatically ticked like they were before.

There is a new information provider "Membership Messages" with a description of ;
'Messages sent from the system owners, VISAV, providing information about member
benefits, asking your opinion about potential new developments and advising you about new
Information Providers.'
The information provider option is on every site and is accessible when logged in, in order to
change/update
The list is customizable for each site

Information providers.

Only licenced *Information Providers* are able to send messages and you control if they are able to see your details or not. This is a list of all the available *Information Providers* in your area and you will only receive messages from and be visible to the ones you select here.

Available information providers

Below are the currently available information providers for you to receive information from. You will only receive information from the information providers you have selected.

☐ Fire & Rescue Service ([More information](#))

The Fire & Rescue Service contributes towards creating a safe and secure community within your county. The organisation strives to inform the people and help prevent fire and road related deaths and injuries.

☐ Get Safe Online ([More information](#))

Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety.

☐ Local Authority ([More information](#))

Local authority messages may include a range of subjects including weather related resilience, scam alerts, rogue trader alerts and emergency warnings.

☐ Neighbourhood Watch ([More information](#))

Neighbourhood Watch trained and licensed administrators (MSAs) assist to keep members details updated, introduce people to schemes and occasionally send messages about Neighbourhood Watch business.

☐ Office of the Police & Crime Commissioner ([More information](#))

PCCs need to communicate with you to check if your policing needs are being met as effectively as possible. They give you a voice at the highest level and make sure their police answer for their actions and decisions. See [here](#) for more information.

☐ SGN (Gas Emergency Service) ([More information](#))

We are the gas emergency service, and we use Alert to provide real time information to our customers in emergencies. The messages SGN will be sending out on Alert will be purely advisory and be extremely useful to Alert users who choose to receive them.

☐ The Police ([More information](#))

The Police means your local Police force and a limited number of personnel from other Police Forces in the UK. They send crime updates, safety advice and requests for information.

☐ Action Fraud (NFI) ([More information](#))

Action Fraud Alert is provided by the National Fraud Intelligence Bureau (NFI) by the City of London Police. They send current scam and fraud notifications with advice on how to stay safe.

Adherence to the obligations of Data Protection

An overview regarding how they are covered within the neighbourhood Alert System.

The UK GDPR sets out seven key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles lie at the heart of our approach to processing personal data within Neighbourhood Alert (Alert) as follows:

Lawfulness, fairness, and transparency

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

All members whose data is stored on Alert have usually followed a process to add themselves (whether on PC or similar device, mobile phone or "kiosk"), in which case they must read and accept the terms and conditions of being on the system and being visible to and receive messages from their selected Information Provider/s; these terms and conditions inform the member of how their data is processed and stored and how they can be removed from the system if they choose to do so.

The members' data can also be added by administrators of the system to whom they have given the relevant information, whether that is by completing a form with their data, on a mobile device held by the administrator or by giving the information verbally to the administrator to input on a device.

All forms of signup state the means of data control and the system provider's and Information Provider's responsibilities to the member and their data. If a member is added by someone else (friend, volunteer, Police officer etc) then the terms and conditions are emailed to the member before the process can be completed. If the new member does not click a confirmation link in the introduction email their temporary record will be deleted entirely from the system within 30 days.

All members are reminded periodically that they are on the system, who can see their information and how they can unsubscribe.

Members can log in to a free, secure account at any time and unsubscribe. They can click a link included on any email message and unsubscribe immediately without the need to log in. They can also contact the support desk on support@neighbourhoodalert.co.uk with a simple request to unsubscribe or reply to any Alert text message with the word STOP and their account will be deleted.

Purpose limitation

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

Members joining the Neighbourhood Alert system are provided with a list of simple, clear concise terms which require agreement before registration on all sites. E.g., <https://member-registration.neighbourhoodalert.co.uk/85/Join>

Member's data is only held for the purpose of them being contacted by one or other of the Information Providers they have chosen to receive messages from. Their data cannot be seen by or used to send messages by any Information Provider that they have not specifically agreed can send them messages.

VISAV maintain a support ticketing system which ensures all incoming communication from members is dealt with promptly and we can identify and escalate priority issues such as miss or inappropriate use of the system swiftly. Members are encouraged and reminded to contact our support desk if they ever receive a communication that feels inappropriate to the purpose with which they joined the system.

All licenced Clients are reminded of the purpose with which they can use the system periodically.

Data minimisation

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

The details recorded by Alert only include information necessary in order to facilitate communication, understand information about a member so messages and support can be relevant to them.

The data collected comprises of basic contact information, demographic details (age, religion, gender etc) and community interest, participation and experience details (Shop Watch, Neighbourhood Watch, First Aid skills etc). This information is gathered from the member during registration and afterwards through a series of relevant surveys.

The data is used to ensure that relevant safety information can be sent and a profile of who is or is not registered can be created in order to ensure underrepresented communities are given the opportunity to have a voice on the system.

Accuracy

(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

When an email address is given at signup the first message received from the system is an email containing a link for the recipient to click to verify we have the correct email address from them; if the link is not clicked the member is flagged as having an unverified email

address, giving the opportunity for administrators to resend the verification email or contact the member to check the email address's validity. If the email address is incorrect it can easily be changed.

In order to ensure that members continue to receive messages tailored to their location and interests it is important that their data remains accurate. If any of their data changes members can update it at any time, either by logging in to their member admin area, or simply by clicking the "change settings" button which appears at the foot of every email message they are sent.

Members can also request changes be made by an administrator by emailing or calling the support team or by using the "reply" facility, in response to an email, voice call or text message they have been sent. Regular survey facilities enable a member to update their account information and keep it accurate simply by answering questions placed within Alert emails. Automatic, periodic notifications remind members about their current details and who they are sharing their details with, they also enable instant, simple updates to be made to these settings.

The member is always in control of the data held for them and can change it at any time. VISAV monitor sample outgoing messages and ensure that they remain relevant to the purpose defined in our terms and conditions and are within the expectations of members.

VISAV survey all members at least once within two years to ensure that they are receiving a service within their expectations. Any anomalies reported are investigated and the information providers informed.

Storage Limitation

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

All Alert data is regularly managed and cleansed as required. Nonresponsive data is removed, and various processes followed to ensure data that is no longer required is removed and deleted in a secure manner as per our data deletion policy.

Groups and community information is reviewed annually and unused group membership which forms profile information is removed.

Deleted data includes members that have unsubscribed, died, moved away from a geographical area we support or data that our processes have identified is no longer active (dead phone numbers and inactive email addresses etc).

Integrity and confidentiality (security)

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

We have implemented a robust network infrastructure in accordance with NCSC GPG8 and GPG13 and are audited to Cyber Essentials Plus, ISO 9001 and IASME Gold standards. The system is hosted in a PASF accredited Data Centre operating to ISO27001 audited processes.

Information/Cyber Security is a board level responsibility and collectively the whole board is responsible for its implementation throughout the organisation as our Cyber Risk Assessment extends beyond IT infrastructure and into all aspects of our culture. The Cyber Security portfolio rests with our Security and Infrastructure Director.

Data is kept in AES2048 Bit encrypted format when in use and at rest, whilst in transit it uses the highest encryption the browser supports, with a minimum of TLS 1.2

Technical security controls are implemented in line with NCSC GPG8 and GPG13 and a full set of RMADS will be provided as part of the contractual process. Breach handling is detailed within the corporate Cyber Risk Assessment and Business Continuity Plan.

Accountability

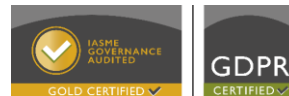
[“The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1”](#)

It should be noted that VISAV cannot use the system for any commercial, promotional means without the written permission of the local force Data Controller. VISAV is specifically prohibited within the licence agreement from communicating with any member of the database for any reason other than system updates and support, service disruption notifications and to periodically remind users who they are sharing their data with.

We derive no income from advertising and could and never would seek to generate any revenue from selling or making member data available. Our business model is licenced services to public authority and privacy and security of data is our core belief.

VISAV is the national Data Controller for the Global Data within the system and as such we accept fully those responsibilities outlined in the above core principles and have fully matured policies that govern this, including Data Protection/Deletion Policies and Subject Access Request Procedure which are checked annually during our ISO audits.

Also, we have achieved the IASME Gold standard which incorporates UK GDPR compliance



How VISA Ltd Implement the NCSC Cloud Security Principles

As a seller of cloud services, we are responsible for understanding your information assurance and security requirements and for assessing how well the suppliers that are chosen can meet them. The NCSC Cloud Security Principles are one of the key tools that help undertake that assessment.

NCSC have released a document entitled *Implementing the Cloud Security Principles* which describes a set of 14 cloud security principles and how they can be implemented.

This following summarises how we implement each of the principles and, where/if appropriate, how we can help you to implement them within your own systems.

Data in transit protection

Principle: Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.

Data in transit and during registration is encrypted to the highest level allowed by the browser using TLS to a minimum of TLS1.2. The network is protected by CAPS approved hardware. We have implemented a robust network infrastructure in accordance with NCSC GPG8 and GPG13

Asset protection and resilience

Principle: Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

a. Physical resilience & availability

Our data centre in Nottingham, which hosts our primary platforms, has a power, cooling and cross connect infrastructure built to the standards of a Tier III + data centre (99.99% availability over a rolling 12month period).

VISA Ltd services are operated solely within UK jurisdiction. All data is held exclusively in the UK.

We are Cyber Essentials PLUS certified and use appropriate management infrastructure, network connectivity, staff security clearances and processes to deliver our services in line with the NCSC Good Practice Guides, DETER protective monitoring and the DPA principles.

Our delivery infrastructure is hosted in our data centre at Space Data Centre in

Nottingham and our secondary (disaster recovery) site is in our Offices in Nottingham.
Access by VISAV staff is role based at permission level required and logged

b. Data Centre security

Our Nottingham Data Centre is certified to ISO27001:2013 and is used to host most of our services. The data centre operates layered physical security controls and 24/7 manned intrusion detection and monitoring.

Our Disaster Recovery (DR) site, which is also used to store off-site backups of customer data, is based in Nottingham and is owned and operated by VISAV Ltd and has CCTV surveillance with access to VISAV Ltd servers limited to appropriate VISAV Ltd staff.

c. Data at rest protection

Physical access to media and storage devices is restricted to VISAV Ltd staff. Data is encrypted, including both data at rest and during on-boarding and off-boarding to AES 256bit

d. Data Sanitisation

VISAV Ltd has a robust customer off-boarding process, covering physical kit, virtual machines, networking configurations and all other aspects of our physical or virtual estate.

All customer data is securely destroyed as part of the off-boarding process

As part of our off-boarding process, existing backups of customer data are usually deleted in line with the agreed data-retention period, however they can be deleted earlier on customer request.

e. Equipment disposal

Our hardware decommissioning process ensures that all decommissioned storage media, with data contained is permanently destroyed as required by (NCSC's) HMG Infosec Standard No. 5

f. Physical resilience & availability

Our data centre in Nottingham, which hosts our primary platforms, has a power, cooling and cross connect infrastructure built to the standards of a Tier III + data centre (99.99% availability over a rolling 12month period).

Our Disaster Recovery service allows for the failover of Managed Infrastructure customer services to our secondary site in the event of a major failure at our primary data centre. This service provides an RPO of 2 hours and an RTO of 24 hours

Separation between users

Principle: Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

Front end servers are separated by geographical portals of police forces.

The data will be separated from other systems using "air-gapped" network infrastructure in line with the former level of IL3 to enable our defence in depth ideology.

Specific administration levels have been created to enable separate levels of access to data using both geographical and company/force hierarchy

Governance framework

Principle: The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Our services and wider business operations have the appropriate management infrastructure, network connectivity, staff security clearances and processes to deliver our services in line with the Cabinet Office Security Policy Framework (SPF) baseline control set at the 'DETER' segment.

VISAV Ltd.'s Board of Directors has delegated direct responsibility for the overall security of VISAV Ltd.'s services to our Security and Infrastructure Director. Risk management for our services is managed using our formally documented Cyber Essentials PLUS accredited processes through daily/weekly/monthly checks each service. Technical compliance checks and protective monitoring at DETER are in place

Operational Security

Principle: The service provider should have processes and procedures in place to ensure the operational security of the service.

a. Configuration and change management

We have a robust and mature change process that is fully integrated throughout all areas of the business asset change lifecycle and that is independently validated as part of Cyber Essentials PLUS

Our Configuration Management File Structure is the central information repository for technical data about all VISAV Ltd configuration items. Change and configuration management activities conducted by VISAV Ltd include:

- i. Logging and scheduling of service requests received via the customer change authority.

- ii. Impact and risk analysis of proposed changes in liaison with relevant 3rd parties, including change approval, security review and regression planning.
- iii. Maintenance of a log of changes; a summary of relevant changes is provided to customers if requested

The perimeter security appliances provide network layer anti-malware protection at a CPU level which extracts unknown malware entering the network. Anti-Spam, Anti Bot and URL filtering are also enabled. Our security devices produce reports on a scheduled basis but can be called up on to run a report at any time.

b. Vulnerability management

As part of our centralised patch management and monitoring process, VISAV Ltd ensures that operating system patches and enhancements are assessed and applied to our management and customer infrastructure in a regular, timely manner with the minimum impact to service. As part of this, we apply routine patch management through automated patch schedules deployed to low impact environments as per our policy

We maintain our situational awareness of new and emerging threats through engagement with vendors (Dell, Microsoft, Juniper, Sonicwall) CertUK, Membership of the CiSP and other specialist groups.

We have adopted a proportionate and prioritised vulnerability management approach based on severity, exposure and compensating controls.

Enterprise grade malware protection is deployed on all devices and is scheduled to scan daily, network security scanning is run to check for patching and security issues using Nessus

c. Protective monitoring

We run protective monitoring against all platforms (covering all the management and customer infrastructure)

Our Managed Protective Monitoring service uses a dedicated individual to provide the setup, configuration and ongoing operation of log monitoring, event analysis and automated alerting in line with NCSC's Good Practice Guide no.13 (GPG-13). All relevant logs are collected, analysed, reported on and archived appropriately.

Any issues identified through protective monitoring are fed into our incident management process.

The perimeter security appliances provide network layer anti-malware protection at a CPU level which extracts unknown malware entering the network. Anti-Spam, Anti Bot and URL filtering are also enabled. Our security devices produce reports on a scheduled basis but can be called up on to run a report at any time

d. Incident management

We operate a well-defined and established ITIL incident management process to log, assign and diagnose incidents based upon urgency and impact (severity/extent) and to restore service operation as quickly as possible with the minimum disruption, in

line with the agreed hours of service and target Incident recovery service level.

Incident management is carried out by VISAV Ltd Information Security team, whose duties include:

- Incident detection and recording – including agreement of Incident priority and logging on incident ticketing system
- Diagnostics, investigation and incident assignment – incident assessment and referral of issues to the relevant resolution team
- Incident recovery – VM reboot or the restoration from backup media of a VM configuration or the implementation of a fix, in line with change management procedures and in conjunction with the customer and relevant 3rd parties
- Call update and escalation – with respect to the target incident recovery service level.
- Critical incident review and monthly security event reviews.

Any incident that runs the risk of jeopardising the integrity of our services is investigated and reported to the VISAV Ltd Information Security team and the appropriate authorities. The first responder principles are applied at the point an incident is detected by VISAV Ltd

Incidents will be managed using VISAV Ltd.'s Information Security Management process and a chain of custody maintained for all evidence collected and preserved. VISAV Ltd will use the services of a professional forensic investigation company, as necessary.

Incidents will be reviewed by the Security Working Group to identify trends and agree any remediation identified, as necessary.

Personnel security

Principle: Service provider staff should be subject to personnel security screening and security education for their role.

VISAV Ltd staff who have privileged roles with respect to customers' information security are vetted to NPPV Level2 by West Midlands Police, any additional vetting is welcomed if required

All VISAV Ltd staff are covered by our disciplinary procedure and staff who have privileged roles with respect to customers' information security are required to sign our and work in accordance with our Administrator Access Rights Policy v1.0.

VISAV Ltd staff receive training and awareness about their security responsibilities.

Secure development

Principle: Services should be designed and developed to identify and mitigate threats to their security.

VISAV Ltd services are maintained and developed in accordance NCSC GPG8 and GPG13 and OWASP Top 10 Vulnerabilities which consider evolving and emerging threats by our Product Developers. Our development is done in-house following development guidelines. All code is developed in an IDE and is held in our version

p
g
.
3
7

COMMERCIALLY SENSITIVE: NOT FOR FURTHER DISTRIBUTION

control systems. Internal testers are responsible for the routine testing of systems and robust release management practices are in place.

Supply chain security

Principle: The service provider should ensure that its supply chain satisfactorily supports all the security principles that the service claims to implement.

VISAV Ltd is not shared or accessible by third parties

All supplies and deliveries are maintained by VISAV and advised from NCSC consultants; all suppliers are subjected annually to the VISAV Ltd Information Security Policy and Supplier Matrix where a minimum of Cyber Essentials is required.

Secure user management

Principle: Consumers should be provided with the tools required to help them securely manage their service.

e. Authentication of consumers to management interfaces and within Support channels

Depending on which services have been purchased, customers may be given access to our platforms' management user interfaces, our platforms' APIs and/or a service desk.

Our platforms' management interfaces are accessed via a web interface. Our service/help desk is available by a web interface, telephone and email.

Customer access to the management interfaces is only provided as role based and is protected using TLS at the highest level the browser supports.

Although access to our service desk is available via both telephone and email, all calls requiring privileged action must be initiated using the web interface Customer passwords are not seen or required by the helpdesk, as they can help to reset using the required process as detailed in our help centre

Access to our platforms' APIs is protected using TLS at the highest level the browser supports

In all cases, we enforce appropriate password complexity rules.

f. Separation and access control within management interfaces

Our platforms' management interfaces use role-based access control and limit functionality to specific user accounts. These roles can be used by customers (and by VISAV Ltd) to tailor functionality to classes of user.

Identity and authentication

Principle: Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

Named user accounts are set up prior to any customer service being made live, with secure information being exchanged out of band.

All access to our platforms' management user interfaces, our platforms' APIs and our service desk is subsequently restricted to that limited set of named accounts.

Access to the platforms' management interfaces is protected using usernames and passwords and can choose their own passwords which are required to be 8 digits alphanumeric
Our protective monitoring service provides alerts and reporting about logins and failed logins.

We have measures in place to deter brute force attacks

Multi-factor authentication is currently is on our development roadmap

External interface protection

Principle: All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them

Weekly external vulnerability scan are performed and issues remedied where required.

We are implementing policies/processes within ISO 27001 framework. We have performed an independent CREST accredited ITHC (results on Police ICT Company Knowledge Hub)

All our cloud services are protected at the network edge by carrier-class next generation firewalls.(CAPS Approved)

Secure service administration

Principle: The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

Our service is underpinned by logically separated management and customer infrastructure. This infrastructure is managed directly from devices which are also used for normal business use (with access controlled as outlined in our responses to principles 9 and 10) and accessed via dedicated VPN and endpoints.

A full ITHC in August 2019 by an independent security company who are CREST providers was performed.

Our Enhanced Segregation service option has also been subjected to a NCSC

p
g
. 3
9

COMMERCIALLY SENSITIVE: NOT FOR FURTHER DISTRIBUTION

design review. If CHECK accreditation is required, that can also be accommodated in the future.

Audit information provision for users

Principle: Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.

We do not currently provide audit information to customers as a standard part of our service infrastructure, we only provide real time audit information on usage of their own portal for administrative and data protection purposes

Secure use of the service

Principle: Consumers have certain responsibilities when using a cloud service for this use to remain secure, and for their data to be adequately protected.

We work extensively with government and third sector organisations, where information security is a primary concern. Security is therefore a key priority across all our operations, ranging from our datacentre, network and cloud infrastructures to our managed services and application development capability.

We have a well-established Service and Security Operations framework, and recommended practice in relevant NCSC Good Practice Guides (GPG-13, GPG-20 and GPG-35).

The key elements of our framework include:

Service support and delivery: consideration of incident management, change and release management; availability management and IT service continuity management

Security Operations: Vulnerability and operation risk assessments. Business Impact Analysis and control; implementations. System access controls and security incident management procedures. Protective monitoring services to DETER Level, including appropriate event log (SIEM) and incident recording, review, analysis, and action regarding threats.

Qamar Sheikh

Security and Infrastructure Director

qamar@visav.co.uk

