Claranet Cyber Security Service Description

# Penetration Testing

**v.6.1**

claranet cyber security®

# Contents





claranet cyber security®

# Service Overview

A Penetration Test involves the use of manual techniques and automated tools to create a controlled simulated attack on predefined targets. Implementing Penetration Testing as part of an information security strategy will allow you to assess the security your organisation's principal assets and identify areas for improvement.

Your engagement will be technically scoped by an experienced Solutions Architect, carefully mapping the target to ensure that the agreed attack surface can be covered during the engagement and that the results are comprehensive within a critical timescale.

The deliverable from Penetration Testing is a report that ranks, in order of risk, exploitable weaknesses and makes recommendations that will assist remediation to ensure that the level of risk is reduced to an acceptable level to the business.

Penetration Testing consists of a wide range of assessment types, from web and mobile applications, infrastructure (both external and internal), devices, social engineering and attack simulations including Red Team.

Penetration Testing is a manual service, delivered as standard remotely between 09:00 to 17:30 hours, Monday to Friday. If the service is required to be conducted outside of these working hours, then additional costs will be chargeable. This document will take you through the diverse options available to you and the stages of the process including responsibilities and obligations for you, our client and Claranet.

Anything not included in this Service Description will not be provided by Claranet as part of the Penetration Testing unless otherwise agreed by the Parties in any Statement of Work (SoW) and/or Order Form together with any additional charges that may be applicable.

---

This Service Description describes the service Claranet Cyber Security provides and details your responsibilities in relation to Penetration Testing. This Service Description forms part of an Agreement between the Parties and is subject to the terms of the Claranet Master Services Agreement set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms.

---

# Scope

Within the Penetration Testing service, the initial Scoping phase ensures that the Claranet Cyber Security Penetration Testing team works closely with you to create a service suited to your specific requirements. This initial phase is to assist in defining an appropriate scope for the test. It may be driven by compliance requirements, best practices, visibility, awareness or a combination of all.

## Initial discussions

Information regarding the scope of the testing can be provided by completing the online Scoping Document on the Claranet Cyber Security Penetration Testing pages. Initial discussions may also take the form of a conference call, face to face meetings or a WebEx. During this stage, we will discuss the challenges and requirements you have and how the test can assist in meeting these. For more complex engagements, it may be necessary to arrange a workshop to tailor the Scoping Document to meet complex requirements and the subsequent development of the detailed Statement of Work.

## Scoping Document

The Scoping Document will need to be completed by you prior to Claranet providing costings and a proposal document. It will allow for a defined Statement of Work (SOW) to be produced along with a prescription of the number of days the engagement will take to complete. Most Penetration Tests can be defined by a set of criteria, such as IP addresses, URLs and applications. These will form the basis of the Scoping Document, which will:

- Identify the drivers and goals for the assessment
- Specify the locations from where the testing will take place if standard remote testing doesn't apply
- Suggest the ideal timescales for your testing
- Define the times of day where testing is permitted or not permitted
- Cover all main targets, enterprise-wide that require assessment
- Clarify the level of access (authenticated or not)
- Allow for the protection of sensitive information stored on the network or within an application
- Detail any exclusions.

### Areas considered during scoping

Testing engagements will be defined by their location, the time of delivery for the assessment (i.e. in-hours or out-of-hours), and the duration of the engagement defined by how many days a tester will need to complete the

assessment based on the appropriate Claranet Cyber Security Methodology for each target. Areas commonly considered during the scoping will include:

- Network infrastructure
- Web applications
- Mobile applications
- Wireless networks
- Routers, switches, laptops, workstations and other devices
- People and processes
- Physical infrastructure.

# Statement of Work

Once the Scoping Document has been completed, the Solutions Architect will examine the information provided and apply a rigorous and consistent approach to ensure that sufficient time is allocated to the engagement to meet the objectives; the result of this exercise is the Statement of Work. The notes added to the Statement of Work are based around how Claranet Cyber Security will complete the testing. e.g. 1 day to test the target, 1 day to report the findings; or Claranet Cyber Security will test the following 5 targets from the list of 30 available in a sampled approach.

Where it is not possible to complete a Statement of Work from the Scoping Document or the information available at the time of scoping, a statement of requirements can be defined and time-based tests can be conducted. However, these may result in an incomplete or inconsistent assessment of the target and require careful consideration and agreement to ensure that expectations are met while maintaining the quality of the service provided.

# Recommendation

Claranet Cyber Security will make recommendations regarding the structure of your assessment and return a Statement of Work to you. Engagements will be defined by the type and complexity of the target(s), their location (standard testing is delivered remotely unless there is a technical reason why the test should be delivered onsite), the time of delivery for the assessment i.e. in-hours or out-of-hours, and the duration of the engagement defined by how many days a tester will need to complete the assessment based on the appropriate Claranet Cyber Security Methodology for each target.

A quote, or proposal document where appropriate, will be provided defining the costs, including any expenses, of the exercise. A sales order form will be produced as a final document for signature.

| Responsibility | Claranet | You |
|---|---|---|
| **Proposal and Statement of Work:** Provide a high level quotation/proposal detailing the structure, price and delivery duration for the engagement and in accordance with the details outlined in the Scoping Document, produce a final Statement of Work and a sales order form for signature. | ✓ | |
| **Scoping Document:** Provide any information required by Claranet relevant to the assessment and in support of a full and exhaustive test. This information will form the basis of the final test, so it is your responsibility to ensure that the information and access provided is accurate, comprehensive and sufficient. | | ✓ |
| **Drivers:** Detail any compliance or industry regulators involved in the assessment. These may have a material effect on the composition of the test, the consultants that are used, and the style of reporting. | | ✓ |
| **Recommendations:** Make recommendations regarding the depth, coverage and type of test, as well as whether a remote delivery is possible, in-line with the desired outcome. | ✓ | |
| **Managing risk:** Identify areas of weakness and or concern that present a risk of system failure and the exposure of sensitive data and then suggest tests to cover these areas. | ✓ | |
| **Exclusions:** Consider any systems that are to be excluded from the assessment, detailing them in the Scoping Document which forms the basis of the Statement of Works. | | ✓ |

# Prepare for testing

The design of your complete Penetration Test depends largely on the scope of the estate to be tested, whether or not it is a remote delivery and the scheduling of the testing.

## Scheduling

Tests can be scheduled upon receipt by Claranet Cyber Security of a Purchase Order. Your Delivery Coordinator can provide an indication of the potential availability of suitable Penetration Testers at any stage. We will work with you to get the test underway as quickly as possible, however, resource availability changes rapidly and the allocation of testers will only be confirmed once a Purchase Order has been received.

| Responsibility | Claranet | You |
|---|---|---|
| **Identify a timescale:** Provide potential timeframes through your Delivery Coordinator for delivery of the work. As the availability of resources changes rapidly, these timeframes are indicative only and cannot be confirmed until a Purchase Order has been received. | ✓ | |
| **Scheduling dates:** Agree the testing dates and ensure that the targets will be available and accessible at the time of testing. | | ✓ |
| **Access:** Provide access details, credentials and supporting information as requested at the time of booking. If an area is under development, you will ensure that the target is populated with data for testing. | | ✓ |
| **Inform stakeholders:** As part of the **Prepare for testing** phase, you will ensure that any stakeholders, including internal and third party, who may be affected by, or want to be aware of, penetration testing activity, are informed. | | ✓ |
| **Reserve and allocate Penetration Testers:** Once the Purchase Order has been received, the dates for your Penetration Test can be confirmed. | ✓ | |
| **Permission to proceed:** Any third parties who host or are connected to your systems, services, or applications, may require notification of the Penetration Test. You agree to obtain any necessary permissions or consents in advance of the Penetration Test commencement. This is particularly relevant for cloud hosting environments. | | ✓ |

## Cancellation and delays

Claranet Cyber Security will allocate the appropriate number of Penetration Testers to your service. In the event of a delay or cancellation before or during the test, the appropriate fee will be payable. Details are in the **Appendix**.

Where a target is not ready for testing or access is not provided prior to the commencement of the engagement, Claranet Cyber Security may decide, for the benefit of all Parties, to delay and reschedule the engagement. Where this is the case, an appropriate rescheduling fee will be applied (see the Appendix).

# Communication

Clear lines of communication are critical to an efficient Penetration Test, covering the transfer of information, how this is achieved, the frequency and the personnel involved. Describing the key personnel on both sides who are responsible for the target environments and the testing, ensures that any issues can be acted upon quickly.

| Responsibility | Claranet | You |
|---|---|---|
| **Contact information:** Provide contact details of the Penetration Testers involved in the service | ✓ | |
| **Contact information:** Provide contact details of those within your company that Claranet are to deal with. In addition, this will include multiple communication channels in the event of an emergency. You will also ensure that these contact details are kept up to date. | | ✓ |
| **Encryption of communications:** All sensitive communication between Claranet and you will be encrypted. Channels available include: PGP, Egress Switch, Encrypted File with out-of-band password sharing. | ✓ | |
| **Update frequency:** Updates on the test progress are available at regular intervals throughout the Penetration Test. You will inform Claranet Cyber Security on your preference in relation to the frequency of these updates, the level of detail you require and consider any potential impact this might have on the time that is available for testing. | | ✓ |
| **Scheduling:** Inform Claranet Cyber Security of any changes to the dates, contact details or targets as early as possible. Changes to dates and targets may result in additional costs. | | ✓ |
| **Scheduling:** Inform you in a timely manner of any changes to dates or to the Penetration Testers involved in the delivery of the testing activity. | ✓ | |

# Providing the authority to test

Providing Claranet Cyber Security with an authority to test is a critical component of testing. At the conclusion of this phase, the targets for testing are confirmed and by ordering with us you are accepting the delivery of Penetration Testing and consent to Claranet Cyber Security performing Penetration Testing activities on these targets.

By authorising Claranet Cyber Security to undertake the testing activities agreed, you are confirming that you have obtained, or will obtain where necessary, the consent of all appropriate parties for testing to be carried out. Claranet Cyber Security will deliver the Penetration Testing in the belief that it has all of the appropriate consents, permits and permissions from you and your companies, as well as employees and sub-contractors where required.

| Responsibility | Claranet | You |
|---|---|---|
| **Authority to test:** Provide any necessary licences, consents, permits, permissions or authorities for Claranet to test the agreed services. | | ✓ |

# Agreement and confirmation

At the conclusion of this phase, the scope of the estate involved, the design of the Penetration Test, and pricing have all been confirmed and agreed.

| Responsibility | Claranet | You |
|---|---|---|
| **Order:** Once completed, you will agree the Scoping Document, the Statement of Work, the Master Services Agreement and the Sales Order Form in order that Claranet can begin testing on the agreed dates. | | ✓ |

# Testing

## Commencement of testing

The testing of your infrastructure and web applications will begin on the dates agreed. This will be against the targets provided by you in the Scoping Document.

| Responsibility | Claranet | You |
|---|---|---|
| **Remote Infrastructure Testing:** Claranet Cyber Security testers will provide a Virtual Machine for you to deploy in the target environment and assist and support during the set-up. | ✓ | |
| **Testing:** Claranet Cyber Security will deliver the testing against the target(s) described in the Scoping Document and aligned with the objectives set out in the Statement of Work on the dates agreed. | ✓ | |
| **Maintain access:** Ensure that access to the target(s) is maintained throughout the testing window. Should access fail, you will act promptly to restore the required level of access to ensure that testing activities can be completed during the dates booked. | | ✓ |
| **Debriefing:** If requested, the Penetration Tester will provide a brief update at the end of each working day. A debrief will be provided upon conclusion of the engagement with a high-level overview of what was found. More information can be found in the **Reporting** section. | ✓ | |
| **Emergency contact:** Ensure that the nominated individual is available to the tester(s) during the engagement to answer any questions relevant to the delivery of the test. | | ✓ |

### Location for testing

Claranet Cyber Security's Penetration Tester will complete the test from a location agreed during the **Scope** and **Prepare for testing** stages and as outlined in the Statement of Work. As a general rule, web application and network infrastructure testing is carried out from our offices or from a secure location. If an onsite delivery is

required, this should be made clear during the scoping stage as this will affect the personnel involved, the scheduling and the price.

In the case of network infrastructure testing, our standard approach is to deliver this remotely using a secure connection to a fully equipped virtual environment deployed within the target network. The feasibility of this will be discussed during the **Scope** phase. Where elements of the attack surface can only be effectively accessed onsite, we will deliver that part of the test at your premises.

### Timing of the manual testing

Manual testing is completed between 09.00hrs and 17.30 hrs, Monday to Friday. Due to the organic nature of testing, there is generally no notification provided as to which areas are being tested at what times, unless agreed and reflected in the Statement of Work.

### Timing of automated testing

Automated tests will be run at any time during the Penetration Testing service parameters. A single automated test or scan may run outside of normal office hours until it is completed and where agreed, will be run overnight to reduce any potential impact it may have on services running as part of normal business operations.

## Methodology

The majority of penetration tests are made against specific infrastructure and application targets. Although every test differs according to specific requirements, the setup of the company, compliance and business considerations and the extent of the estate affected, there is a commonality of operations across them.

The first stage of a Penetration Test will begin by gathering information on the target and making an initial vulnerability assessment. This can be carried out with an automated procedure. Once obtained, a manual process of analysis and identification of an exploitation path is made. These are then thoroughly investigated by an experienced Penetration Tester and an attack process is created to determine the extent of the vulnerability found.

| Responsibility | Claranet | You |
|---|---|---|
| **The finding of all vulnerabilities:** Act in accordance with, and bounded by, the Scoping Document and Statement of Work. Consequently, it cannot be guaranteed that all vulnerabilities will be found or exploited to the full. Claranet Cyber Security will use our best endeavours to locate and exploit vulnerabilities within the scope but is not responsible for any attacks through vulnerabilities that have not been identified. | ✓ | |

This continues across all targets determined in the Scoping Document and agreed in the Statement of Works. There are individual Claranet Cyber Security Methodology documents covering each specific area, and the appropriate one is available upon request from your Account Manager.

# Handling of sensitive data

Part of the objective of a Penetration Test is to assess the risk to sensitive information or to compromise high-value digital assets. Contact with potentially sensitive information is common and therefore will be managed accordingly. Where possible, Penetration Testers avoid coming into the possession of Personally Identifiable Information.

Validating the presence of a vulnerability ensures accuracy in the reported results of a Penetration Test. Proving that a vulnerability exists within the systems containing sensitive data is achieved in a number of ways, for example; obtaining screenshots of database schemas and file permissions, or displaying files without displaying the contents.

Further to these measures, encryption on Penetration Tester machines protects any data or information we do come into contact with and regular scrubbing of devices ensures that data is not retained.

| Responsibility | Claranet | You |
|---|---|---|
| **Sensitive data:** Act in accordance with the Claranet Cyber Security practice for handling of your sensitive data and general best business practice. Penetration Testers will, where possible, avoid coming into the possession of Personally Identifiable Information. | ✓ | |

# Review

## Reporting

Once testing activities are complete, a report is produced which includes:

- Executive summary
- Graphical summary
- Overview of vulnerabilities
- Technical analysis

### Executive summary

This provides a high level summary of the key findings of the Penetration Test. The results are provided in context. (e.g. in order to exploit this vulnerability a hacker would have to be connected to the internal system). This section includes any constraints and restrictions of the test.

### Graphical summary

This provides a graphical view of the number of high, medium and low rated vulnerabilities measured against risk categories or impact and probability.

### Overview of vulnerabilities

A section that concentrates on high and medium vulnerabilities. Low vulnerabilities are included here if it is necessary or they prove indicative of a more serious issue.

### Technical analysis

The technical reporting is presented in order of risk, with high risk vulnerabilities appearing first. Full details are provided which include:

- Exploitation path
- Screenshots and Proof of existence (e.g. a vulnerability is found but the exploitation is theoretical, e.g. a website is not actually taken down
- Remediation recommendation

# Quality Assurance

At the completion of a report, it is passed through a Quality Assurance process within Claranet Cyber Security where it is reviewed by senior colleagues. Any amendments or changes that are suggested are then fed back to the Penetration Tester(s) that are involved in the delivery of the test so that these can be applied.

It is then sent directly to your nominated contact(s) in the Scoping Document by the pre-agreed and appropriately secure method.

Full final reports are completed within 10 working days, though larger projects that require multiple reports or those with large volumes of results to report may take longer. Where this is the case, if it can be identified and communicated during the **Scope phase** then interim results and draft reports can be provided to ensure that remediation activity is not delayed. Where results are required by a specific date, this needs to be agreed during the **Scope phase**.

# Common Vulnerability Scoring System (CVSS)

Each vulnerability that is found is measured against CVSS. This provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploitation with the impact of exploitation.

The numerical score can then be translated into a qualitative representation (such as 1 = low, 5 = medium, 10 = high) to help you properly assess and prioritise your vulnerability management process. This universal measure reduces the subjective analysis between one tester and another.

# Timescales

The length of time spent producing the report is determined at the **Scoping** and **Prepare for testing** stage and will usually be booked as close to the completion of testing as possible.

Where a final report is needed by a specific date, you must inform Claranet Cyber Security as early as possible so this can be accommodated. We will make all reasonable endeavours to accommodate the request and will discuss these with you at the **Scoping** and **Prepare for testing** stage. This is to ensure that adequate resource can be assigned to the production of your reports at the specified time.

Additional options are available to ensure that results and associated remediation is understood and agreed e.g. a discussion between your stakeholders and the Penetration Testing team can take place either onsite or remotely in order to explain what was done during testing and to identify any remediation required to remove or downgrade the risk.

# Retesting

Following a period of remediation, there may be a requirement for retesting of the vulnerabilities found, to validate that the fixes have been successful in addressing the risk. This is a chargeable exercise and will be discussed at the **Scope** and **Prepare for testing** stages. Once the results from the initial test are identified, this can be

discussed again in order to determine the potential benefit and timescales. Where remote testing has been delivered, it will be possible to organise cost-effective retesting of the target infrastructure to validate the remediation.

| Responsibility | Claranet | You |
|---|---|---|
| **Accuracy of reporting:** Apply a rigorous Quality Assurance process to ensure that the results reported are as precise a reflection of the risk as possible. | ✓ | |
| **Delivery of reports:** Deliver a report as soon as possible following the completion of the testing activities. This will contain an Executive Summary and an Overview of vulnerabilities. The exploitation detail will be ranked in order of risk and in accordance with the CVSS. | ✓ | |
| **Following up reports:** Make available testers for remediation discussions. This can be discussed during the Scope and Prepare for testing stage or can be organised through your Account Manager. | ✓ | |
| **Retesting:** Discuss any potential retesting requirement through the Account Manager and can suggest timescales and objectives of this activity. | ✓ | |
| **Retesting:** Decide what retesting is going to be required and to discuss this with the Account Manager or the Penetration Testing team to ensure that any commercial and scheduling considerations are fully taken into account. | | ✓ |
| **Receiving reports:** Provide contact details (email and mobile phone number) for the individual who is to receive the report. This must be provided at the outset of the testing and should be included in the Scoping Document. You will also maintain the list of current contacts in the event of changes from the original list. | | ✓ |
| **Following up reports:** Decide what type of assistance (if any) will be required to understand and apply the most effective remediation based on the findings of the Penetration Test. Advice may also be required to reduce the risk of compromise to the main target system(s). | | ✓ |

# Feedback

Claranet strives to continuously improve the services offered to its customers and one of the key ways that we achieve that is by listening. We would love your feedback on how we performed before, during and after the

engagement and any suggestions you may have to help us to improve the service. Your opinions are important to us so please complete the short feedback survey below;

Customer Feedback Form

# Appendix

## Service terminology

Throughout the document or in association with it, a number of terms have been used. These can be found in the general description below.

- **Device Penetration Testing;** including workstations, laptops, routers and consumer devices (e.g. tablets and smartphones)
- **Infrastructure Penetration Testing**; examines servers, firewalls and other network components for security vulnerabilities that could be exploited
- **Manual Penetration Testing**; a generic term for assessments using manual techniques to simulate an attack on your systems
- **Mobile Application Penetration Testing**; looking for exploitable weaknesses in mobile applications
- **Penetration Test or Testing;** typically an assessment of IT infrastructure, networks and business applications to identify attack vectors, vulnerabilities and control weaknesses. When executed properly, a Penetration Test will describe weaknesses in your technical security and provide the information and support that you need to remove or reduce the risk that the vulnerability causes. Claranet Cyber Security provides a range of options for Penetration Testing, covering your applications to your underlying infrastructure. Undertaking a series of Penetration Tests will help you assess your organisation's risk in the face of an attack and help to identify improvements.
- **Red Team Exercises**; usually an attempt to achieve agreed objectives by any legal means possible using a combination of the above attack simulations and where the target organisation actively defends
- **Remote Infrastructure Penetration Testing**: full coverage of an Infrastructure Penetration Test but delivered remotely rather than a tester coming on site
- **Social Engineering**; attempting to gain information or access by deceiving employees in the same way that an attacker would
- **Test Report;** a document produced at the end of a Penetration Test that contains details of the vulnerabilities found ranked in order of risk, how they might be exploited and suggested remediation.
- **Vulnerability Assessments**; using only automated tools to identify common vulnerabilities
- **Web Application Penetration Testing**; an authenticated or non-authenticated manual test against Internet-facing applications or application-based business systems

- **Wireless Penetration Testing;** a security assessment of WiFi networks and whether they could provide an access point to corporate data

The components of the Claranet Penetration Testing portfolio are supported by a set of documented testing methodologies, which are available on request.

# Fees, payment and legal

Fees payable under this Contract will be invoiced on delivery of the Test Report or, if no report is to be provided, on completion of the Penetration Testing.

If ordered days not paid for up-front are not used within 12 months, then Claranet Cyber Security will invoice the days. You will then have 6 months to schedule the days.

## Delays and cancellations

Immediately following the agreement of dates for the Penetration Testing service to begin (and the receipt of any purchase order as applicable), Claranet Cyber Security will start to allocate resources and facilities and will therefore commit to any third party expenditure to fulfil its contractual commitments. Claranet Cyber Security may at its absolute discretion allow the Penetration Testing to be re-scheduled or cancelled. If this occurs, you agree that you are committed to paying Claranet Cyber Security a proportion of the fees as pre-estimated liquidated damages. In the case of late notice rescheduling, this fee will be in addition to the full price for the engagement which will be invoiced upon delivery of the Test Report. This will reflect the losses which Claranet Cyber Security will incur due to the cancellation or re-scheduling.

These proportions are as follows:

| Cancellation timescale | Cancellation fee (% of engagement price) |
|---|---|
| Cancellation request received more than 30 working days prior to start date. | 25% payable |
| Cancellation request received 8 to 30 working days prior to start date. | 50% payable |
| Cancellation request received within 7 working days of start date. | 90% payable |

| Reschedule timescale | Reschedule fee (% of engagement price) |
|---|---|
| Re-schedule request received more than 30 working days prior to start date. | 0% payable |
| Re-schedule request received 8 to 30 working days prior to start date. | 25% payable |
| Re-schedule request received within 7 working days of the start date with a firm re-booking date. | 50% payable |

### Unavoidable absence

Should a tester allocated to your Penetration Test become unavailable at short notice for reasons that are commercially unavoidable (for example; sickness) then every attempt will be made to provide a replacement at the earliest possible opportunity. In these circumstances, whilst some delay is usually inevitable, Claranet Cyber Security will endeavour to minimise the impact on the delivery of the results.

### Travelling

For onsite work, Account Managers and Penetration Testers will plan the schedule of the test to take into account travel time. Clients are not normally charged for time incurred during travelling (only the cost of the travel), to maximise the available testing time, some engagements may start at any time up to midday. Where this is the case, your Account Manager will discuss and agree the options that are available. Where travel delays are incurred the tester will contact you to provide an estimated time of arrival. Where possible the tester will make up any time lost by travel delays during the engagement.

### Billing

Where you order Penetration Testing day units and do not allocate or use these within twelve months, Claranet Cyber Security will invoice you for these days at our convenience on or about the twelfth month, whether or not you allocate the days at that time.

### Expenses

Expenses are charged at cost for travel, accommodation and sustenance where onsite work is required. Your Account Manager can provide you with an estimate of any likely expenses during the **Scope** stage. To ensure accuracy and the lowest costs possible, expenses are charged upon completion of the Test unless otherwise agreed.

## Boundaries of the service

Conducting the Penetration Tests involves the testing of your live systems on your current infrastructure. This may therefore have an impact on current workloads and environments and these will be discussed with you prior to commencement and minimised wherever possible. To this end, you will appoint at least one employee who shall act as liaison between yourselves and Claranet Cyber Security. They must have substantial experience of your computer systems, networking and project management of your information systems.

| Responsibility | Claranet | You |
|---|---|---|
| **Operational involvement:** No intentional interference will be caused to the operation of your information system, unless it is with your express authority. | ✓ | |

| | |
|---|---|
| **Boundary violations:** Inform you of any violations of any test boundaries that occur. In the event of any boundary violation, Claranet Cyber Security will cease testing, document the extent of the violation and inform you as soon as is practicable. | ✓ |
| **Liaison:** Provide an employee as liaison with Claranet Cyber Security that is technically familiar with your systems as described. | ✓ |

# Reclassification of the scope

Changes to systems already included within the scope for Penetration Testing may require the system to be re-scoped according to the target complexity levels. Targets may increase or decrease in size. Changes to the scope may incur an additional cost.

# Terms used in vulnerability reporting

The terms used within any vulnerability notification messages are listed below:

| Description of the term | Rating |
|---|---|
| **Vulnerability impact**<br>An estimation of the potential business impact if the vulnerability was exploited. | High / Medium / Low |
| **Vulnerability probability**<br>Probability is defined by the complexity and likelihood of exploitation. | High / Medium / Low |
| **Vulnerability description**<br>A technical description of the vulnerability and potential exposure. | |
| **Technical analysis**<br>A description of the work required to validate the vulnerability including proof of concept, screen shots and steps required to reproduce the finding. | |
| **Remediation**<br>A description of the actions required to implement a successful fix to the vulnerability. | |

# Legal obligations

By signing the Sales Order form:

1. You have procured, and acknowledge Claranet Cyber Security is relying upon your obtaining of any necessary consents as required of your (and your group companies') employees, agents and sub-contractors for the Penetration Testing to take place;
2. You hereby give permission to Claranet Cyber Security to access the various IT systems which may be affected by the Services delivered pursuant to the Statement of Work;
3. You have informed and gained consent where appropriate of any interested parties, individuals, users, third party information stakeholders, third party information service providers or any other parties likely to be affected by the Penetration Testing carried out by Claranet Cyber Security of the planned Penetration Testing, the likely and potential impact and how this may affect them directly, the date and time of the Penetration Testing;
4. You confirm that you have obtained all consents required from data subjects to enable personal data (as defined in applicable data protection legislation) to be disclosed to Claranet Cyber Security to the extent required to carry out the Penetration Testing;
5. You confirm the carrying out of the Penetration Testing does not contravene any law or regulation in so far as it relates to individuals, users, third party information stakeholders, third party information service providers or other parties likely to be affected by the Penetration Testing on your information systems;
6. You agree that, in accordance with The Computer Misuse Act (1990), you will provide where appropriate, all necessary authorisations for access to target systems to Claranet Cyber Security, including, where necessary, modifications that demonstrate the impact of exploitation of a vulnerability.
7. You agree to take all reasonable measures to protect your information system from any loss or damage that may arise as a consequence of the Penetration Testing. Prior to commencement of the Penetration Testing, you will take copies of information and applications or use any other methods available to them, to ensure the safety and protection of material within the information system. Claranet Cyber Security shall not be liable for any data loss including that which cannot be recovered due to inadequate back up or protection by you.
8. You agree that, where the Penetration Testing is to take place on your premises, you shall ensure that a suitable working environment is provided for the Claranet Cyber Security Penetration Tester which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms.
9. You agree that should you require a laptop or other device to be security tested by Claranet Cyber Security at our offices you will deliver the laptop and/or other device to Claranet's designated office and collect it from those offices or authorise other means of delivery and return at your own risk. Claranet Cyber Security shall not be liable for the laptop, device, or PDA during transit to or from its offices.

10. You agree to provide Claranet Cyber Security with at least one employee who has substantial computer systems, network and project management experience of your information system to act as liaison between you and Claranet Cyber Security.
11. You agree to co-operate with Claranet Cyber Security and to provide it promptly with such information about your information system, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by Claranet Cyber Security to perform the Penetration Testing.
12. You confirm that, where the Penetration Testing is taking place on your premises, the premises are safe in line with current Covid-19 guidelines, suitable and reasonable to accommodate Claranet Cyber Security's Penetration Tester and the Penetration Testing.
13. You agree that copyright in the test report(s) received by you in relation to the Penetration Testing shall remain the property of Claranet Cyber Security, and that Claranet Cyber Security, upon receipt of payment in full, hereby grants you a non-exclusive, non-transferable licence to copy and use the contents of those test reports for your own internal purposes only.

# CHECK scheme testing

Claranet can deliver testing under the conditions set out by the National Cyber Security Centre's CHECK scheme. More information is available here;

https://www.ncsc.gov.uk/section/products-services/ncsc-certification

Where this is required, clients should make their account manager aware as soon as possible in the scoping process so that CHECK specific administration can be arranged and appropriately authorized CHECK Team testers assigned.

**Information control and feedback**

NCSC may contact clients using the CHECK scheme to request information regarding the performance of Claranet in delivering the service. Where this is the case, any information shared with NCSC will be for quality control only and not forwarded to any other organization without the express written permission of the client.