

Vulnerability Disclosure Policy

Utility Warehouse

January 2026

Contents

Introduction	3
Scope	3
Reporting	3
Philosophy and Guidelines	4
Legalities	6

Introduction

The vulnerability disclosure policy defines the process and expectations when reporting vulnerabilities to Utility Warehouse (UW) Limited, Telecom Plus PLC, and subsidiaries (“us”, “we”). We would recommend that you read this policy fully before reporting a vulnerability to us, and always act in accordance with this policy.

We define a security vulnerability as an unintended weakness or exposure that could be used to compromise the integrity, availability or confidentiality of our products and services.

Scope

This policy applies to anyone that investigates and/or discloses a vulnerability to us, within technology assets or processes that are owned, operated or maintained by us, including public facing websites.

Reporting

If you have discovered a security vulnerability, please report this to us by emailing security@uw.co.uk . Our PGP public key can be found on the [Forum of Incident Response and Security Teams \(FIRST\) website](#) , please always use this if you are sending us confidential information. If you’re unsure of how, first email us without any confidential information and we’ll provide you with some guidance.

In your report, please include:

- The location of the vulnerability (website page or IP address);
- A brief description of the type of vulnerability (e.g. “SQL Injection”);
- Steps that we can follow to reproduce, as a non-destructive proof of concept.

We will acknowledge receipt of each vulnerability report, conduct a thorough investigation and then take the appropriate action for resolution. We ask that you do not share any vulnerabilities with anyone other than us (through the email address above). This gives our teams the opportunity to thoroughly investigate and resolve the problem.

Philosophy and Guidelines

We believe that effective disclosure of security vulnerabilities requires mutual trust, respect, transparency and common good between us and you. Together, our attentive expertise supports the continued security and privacy of our customers, products, and services.

This philosophy is supported by guidelines that must be followed to ensure that vulnerability investigations and disclosures are safe and conducted without causing unnecessary harm.

Our Commitment to Researchers

Trust . We maintain trust and confidentiality in our professional exchanges with security researchers.

Respect . We treat all researchers with respect and recognise your contribution for keeping our customers safe and secure.

Transparency . We will work with you to validate and remediate reported vulnerabilities in accordance with our commitment to security and privacy.

Common Good . We investigate and remediate issues in a manner consistent with protecting the safety and security of those potentially affected by a reported vulnerability.

What We Ask of Researchers

Trust . We request that you communicate about potential vulnerabilities in a responsible manner, providing sufficient time and information for our team to validate and address potential issues.

Respect . We request that researchers make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing.

Transparency . We request that researchers provide the technical details and background necessary for our team to identify and validate reported issues, using the form below.

Common Good . We request that researchers act for the common good, protecting user privacy and

security by refraining from publicly disclosing unverified vulnerabilities until our team has had time to validate and address reported issues.

Guidelines

You must NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in our systems or services.
- Use high-intensity, invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt our services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in this policy or the published security.txt.
- Social engineer, ‘phish’ or physically attack our staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

You Must:

- Always comply with data protection rules and must not violate the privacy of our users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being reported, whichever occurs first (or as otherwise required by data protection law).

Legalities

We intend for this policy to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us to be in breach of any legal obligations.