

INFORMATION SECURITY STATEMENT

Information security at Bunzl is governed by our Global Information Security Policy. We have a multi-layered approach to network and email security from firewalls, servers through to workstation protection and work with best of breed security partners, and vendors, who provide us with the necessary knowledge, tools and technology to support our multi-layered security and network architecture.

We have implemented a blend of controls using people, processes and technologies from industry leading suppliers. We actively monitor these controls to ensure their effectiveness and to highlight deficiencies and highlight improvements.

Patching is undertaken routinely and we have a dedicated security team responsible for infrastructure and applications. We conduct weekly antivirus scanning of servers and workstations and regular penetration tests and security audits.

Our systems are hosted by a secure Tier 3/4 data centre provider and are backed up and tested regularly. Our data retention policy requires us to securely store backups for a minimum of 7 years. Business continuity plans exist in each of our businesses.

Access to our systems is a role based model using least privileged principles, all users are provided with unique access ID's and passwords that are changed regularly. We monitor and routinely check access control lists for accuracy and appropriateness.

We take the security of our customer data very seriously, it is never shared with any 3rd parties and only used appropriately.

We are working with our Security partner towards Cyber Essentials Plus accreditation, which we expect to achieve by the end of 2017.

CLASSIC



This is to certify that

Bunzl PLC

1 Hook Rd, Epsom. KT19 8TY

Has been assessed

by Victor Van der Helm for MTI Technology Ltd
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials

Scope: Cyber Essentials Stage 1 for Bunzl PLC, Bunzl UK Ltd, Bunzl Retail and Healthcare Supplies Ltd, Bunzl Ireland Ltd

Certification date: May 21st, 2020

Recommended re-assessment date: **July 1st, 2021**

Certificate no.: 4135043363297665



This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

