ABOUT THIS POLICY

This document provides a broad overview of the high-level controls and framework that The Restaurant Group has in place to protect TRG's networks and systems from attacks by malicious actors.

This policy sets out the systems and processes in place for TRG's directly controlled UK operations. Individual divisions or brands may choose to adopt further policies and procedures, or implement additional requirements, provided they are not inconsistent with this policy.

PRINCIPLES

The following principles and processes underly TRG policy:

- Cybersecurity is reviewed periodically using an established framework
- Regular audits are conducted to maintain the control state and coverage required
- External and internal third-party penetration testing is conducted annually to assure the effectiveness of our controls
- Perimeter, network, endpoint and identity and access management controls are in place, maintained and reported on through established processes and services
- Patching, threat and vulnerability management policies are established
- A cyber incident response policy and plan is in place covering the response and approach for dealing with critical cyber incidents.
- Regular staff security awareness training
- Vendor risk management reviews are undertaken when onboarding any new suppliers and systems
- Disaster recovery restore testing is carried out periodically

POLICY COMPLIANCE

Compliance with TRG policies and procedures is mandatory for all TRG staff. Any breach of this policy must be reported to the Cyber Security Manager as soon as possible. This reduces wasted resources spent on investigations and helps develop better controls.

Any non-compliance with this policy will be investigated. Corrective action will be taken where deemed necessary, by senior management and the relevant stakeholders, as part of a continuous service improvement programme.

Non-compliance with TRG policies and procedures could result in disciplinary action being taken against an individual in accordance with their contract of employment and relevant disciplinary policies.

EXCEPTIONS

It is recognised that some activities conducted within TRG may require exceptions to this policy.

Where there is an explicit business need for derogation from the policy, this shall be formally reviewed and any approvals recorded. A copy of the authorisation shall be kept by the user.

The requirements should be reviewed at least annually and the users that are covered by the exception shall notify the Cyber Security Manager in writing when the exception is no longer required.

Drafted: July 2024
Approved by the TRG Board: 30 July 2024