Zapp AG, Zapp-Platz 1, 40880 Ratingen

To all customers of companies of the
Zapp Group

Zapp AG
Zapp-Platz 1
40880 Ratingen
Phone +49 2102 710-0
Fax +49 2102 710-200
www.zapp.com

Chairman of the
Supervisory Board:
Dr. Manfred Puhlmann

Executive Board:
Dr. Stefan Seng
(Chairman),
Gerald Zwickel

Registered Office:
Ratingen
Legal Form:
Aktiengesellschaft
County Court Düsseldorf
HRB 44176

Contact: Dr.-Ing. Wolfgang Püttgen, Quality Management
Phone +49 2102 710-123, Fax +49 2102 710-6123, wolfgang.puettgen@zapp.com

02 February 2022]
Cyber Security and Information Technology Security

Dear Sir or Madame,

You have recently requested information regarding our cyber- and information technology security. At Zapp, we strive to ensure the highest and most economically justifiable level of security for our business operations.

Please understand that, due to the sensitive nature of this matter, we may be unable to answer all of your detailed questions. Nevertheless, we would like to meet your request for information regarding this matter and can therefore confirm the following:

We use the following technologies to protect our IT infrastructure:

- Secured company network (VPN),
- Redundant network connection of all locations,
- Latest routers and firewalls,
- Cascading of firewalls from different manufacturers,
- Detection of network traffic anomalies,
- Segmented networks, especially for production facilities,
- Virtual Domains (VDOM),
- Server virtualization,
- Centralized asset, license, and application management,
- Mobile Device Management (MDM),
- Separation of backup systems,
- Offline backup with media break,
- Data center access controls,
- UPS and backup diesel,
- Two-factor authentication for access to the corporate network,
- Anti-virus protection on all Microsoft endpoints and servers,
- Hard disk encryption on all laptops,

- Next Generation Anti-Virus Protection,
- Incidence Response Service,
- Security Information and Event Management (SIEM),
- Data Access Control,
- Network Access Control (NAC),
- DOS and DDOS Protection,
- Privileged Identity Management (PIM),
- Email Protection:
    - Phishing Mail and SPAM Detection,
    - URL Filtering,
    - Internal Mail Defense,
    - Sandbox Analysis,
    - Anti Spoofing Modules (DKIM and SPF),
    - Domain-based Message Authentication, Reporting and Conformance (DMARC),
    - Thread Response Auto Pull (TRAP).

Furthermore, we regularly implement the following measures:

- Two-tier system/network monitoring,
- Internal and external penetration tests,
- Data backup,
- User awareness training,
- E-learning courses on cyber security,
- Hardening of all relevant IT systems,
- Regular renewal of hardware,
- Permanent patching of the systems,
- Health checks of all relevant systems,
- Disaster response plan,
- Documented emergency concept, crisis management and restart procedures,
- Risk analyses,
- Vulnerability management,
- ITIL processes in IT management,
- Regular coordination with management on security topics,
- Technical organizational measures (TOM) from the DSGVO,
- Coordination with the data protection officer.

In this context, we also seek advice and assessment from external consultants and service providers, specifically:

- IT audit as part of the annual audit by Rödl & Partner,
- IATF 16949 (information technology) by Intertek.

If you have any further questions, please do not hesitate to contact us.

Yours sincerely

Dr.-Ing. Wolfgang Püttgen
Beauftragter Qualitätsmanagement

Dr. Rainer Schmitz
Beauftragter IT-Security